

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-209231

(43)Date of publication of application : 28.07.2000

(51)Int.Cl.

H04L 12/28  
G06F 13/00  
G06F 13/14  
H04L 12/56

(21)Application number : 11-317217

(71)Applicant : RICOH CO LTD

(22)Date of filing : 08.11.1999

(72)Inventor : MATSUDA TORU  
KURT PIASORU  
TERAMURA SHINSUKE  
URABE AKIO  
INAGAKI TATSUYA

(30)Priority

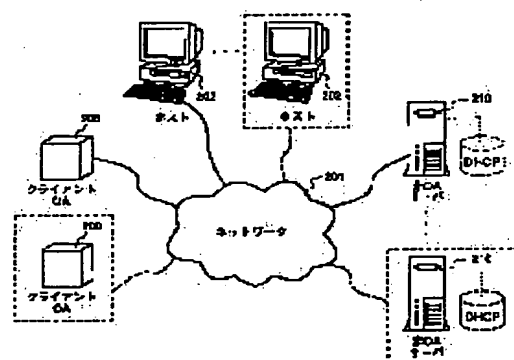
Priority number : 98 191277 Priority date : 12.11.1998 Priority country : US

**(54) DEVICE INITIALIZING METHOD, NETWORK INFORMATION AUTOMATIC ASSIGNING METHOD, NETWORK AUTOMATIC INITIALIZING METHOD, SERVICE AUTOMATIC DISCOVERING METHOD AND NETWORK**

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a comfortable automatic configuration function by requesting configuration information from a second device, when the first device is connected, executing delaying for an optional period before a decision that information is not obtained and executing configuration service in a network, when response is received during the period.

**SOLUTION:** When a bootstrap sequence is started, a client OA200 tries to obtain configuration information required on the network 201. The client OA200 executes broadcasting over the whole network at every time interval through the use of a DHCP protocol. The client OA200 continues broadcasting until either another DHCP OFFER is received or a preset time elapses, transmits DHCP REQUEST to a non-OA server 210, and requests configuration information.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-209231  
(P2000-209231A)

(43) 公開日 平成12年7月28日 (2000.7.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 D
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 V
	13/14		3 3 0 A
H 0 4 L 12/56	3 3 0	H 0 4 L 11/20	1 0 2 A

審査請求 未請求 請求項の数30 O L (全 27 頁)

(21) 出願番号 特願平11-317217  
(22) 出願日 平成11年11月8日 (1999.11.8)  
(31) 優先権主張番号 09/191277  
(32) 優先日 平成10年11月12日 (1998.11.12)  
(33) 優先権主張国 米国 (US)

(71) 出願人 000006747  
株式会社リコー  
東京都大田区中馬込1丁目3番6号  
(72) 発明者 松田 透  
東京都大田区中馬込1丁目3番6号 株式  
会社リコー内  
(74) 代理人 100089118  
弁理士 酒井 宏明

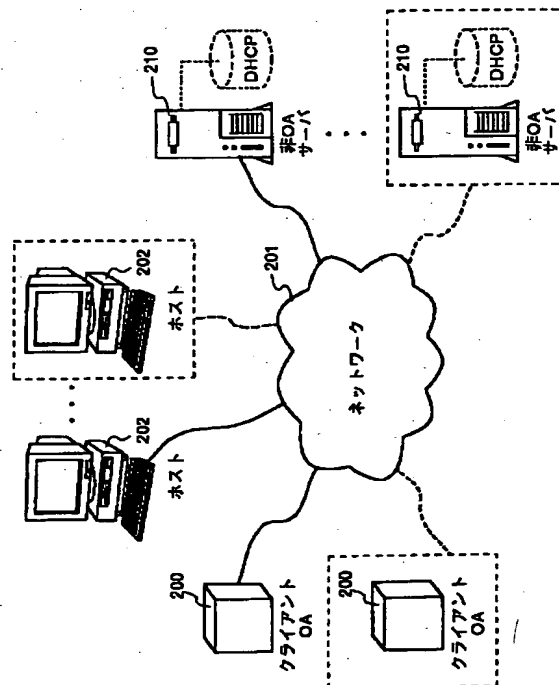
最終頁に続く

(54) 【発明の名称】 デバイス初期化方法、ネットワーク情報の自動割り当て方法、ネットワーク自動初期化方法、サービス自動発見方法およびネットワーク

(57) 【要約】

【課題】 簡単、快適、および家電品のような自動コンフィグレーション機能をユーザに提供するネットワークデバイスを提供すること。

【解決手段】 ネットワークアドレッシング、ネットワークネーミング、サービスディスカバリおよびあるシステムにおけるユーザ識別を提供するネットワークに接続されたオフィス機器で構成された動的に可変なネットワークアーキテクチャである。このネットワークアーキテクチャは、管理されていないネットワークに自動コンフィグレーションサービスを提供し、一方、管理されている環境には自動的に適応することができる。



## 【特許請求の範囲】

【請求項1】 ネットワーク上の第1のデバイスを自動的に初期化するデバイス初期化方法であって、前記ネットワークに前記第1のデバイスを接続すると、第2のデバイスからのコンフィグレーション情報をリクエストする工程と、コンフィグレーション情報を取得できないと決定する前に、任意の期間遅延させる工程と、前記期間内に前記第2のデバイスから前記コンフィグレーション情報のリクエストに対する応答を受信しなかった場合に、前記ネットワークにコンフィグレーションサービスを提供する工程と、前記第1のデバイスが前記第2のデバイスより高い優先順位を有している場合に、前記ネットワークに前記コンフィグレーションサービスを提供する工程と、さらなるデバイスが前記ネットワークに接続されたことを検出するために前記ネットワークを連続的にモニタする工程と、を含むことを特徴とするデバイス初期化方法。

【請求項2】 前記コンフィグレーションサービスを提供する工程は、第1のネットワークアドレスを自動的に決定する工程と、第2のネットワークアドレスを自動的に割り当てる工程と、ネットワーク名を自動的に割り当てる工程と、前記第1のネットワークアドレス、前記第2のネットワークアドレスおよび前記ネットワーク名を自動的に関連付ける工程と、前記関連付けられた第1のネットワークアドレス、前記関連付けられた第2のネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、を含むことを特徴とする請求項1に記載のデバイス初期化方法。

【請求項3】 前記第1のネットワークアドレスは、MAC (media access control) アドレスを含むことを特徴とする請求項2に記載のデバイス初期化方法。

【請求項4】 前記第2のネットワークアドレスは、IP (Internet Protocol) アドレスを含むことを特徴とする請求項2に記載のデバイス初期化方法。

【請求項5】 前記ネットワーク名を割り当てる工程は、ネットワーク名の競合を検出する工程と、前記ネットワーク名の競合を解決する工程と、前記ネットワーク名の競合を示すコードを前記テーブルに記録する工程と、を含むことを特徴とする請求項2に記載のデバイス初期化方法。

【請求項6】 前記ネットワーク名は、前記第1のデバ

イスによって提示されるものであることを特徴とする請求項2に記載のデバイス初期化方法。

【請求項7】 前記期間は、競合状態を防ぐために異なることを特徴とする請求項1に記載のデバイス初期化方法。

【請求項8】 ネットワークアドレスをデバイスに割り当てる工程と、ネットワーク名を前記デバイスに割り当てる工程と、前記ネットワーク名を前記ネットワークアドレスに関連付ける工程と、前記割り当てられたネットワークアドレスから独立している前記割り当てられたネットワーク名でユーザが前記デバイスを参照することができるように、前記関連付けられたネットワーク名および前記関連付けられたネットワークアドレスをテーブルに記録する工程と、を含むことを特徴とするネットワーク情報の自動割り当て方法。

【請求項9】 前記ネットワーク名を割り当てる工程は、前記ネットワーク名が既に使用中の場合、ネットワーク名の競合を解決する工程を含むことを特徴とする請求項8に記載のネットワーク情報の自動割り当て方法。

【請求項10】 前記ネットワーク名は、前記デバイスによって提示されるものであることを特徴とする請求項9に記載のネットワーク情報の自動割り当て方法。

【請求項11】 前記ネットワークアドレスは、DHCP (Dynamic Host Configuration Protocol) を使用して割り当てられることを特徴とする請求項8に記載のネットワーク情報の自動割り当て方法。

【請求項12】 ネットワークを自動的に初期化するためのネットワーク自動初期化方法であって、前記ネットワーク上のデバイスにアドレスを自動的に割り当てる工程と、

前記ネットワーク上の前記デバイスにネットワーク名を自動的に割り当てる工程と、前記ネットワーク全体にユーザおよびグループ情報を自動的に提供する工程と、

前記ネットワーク上の前記デバイスが実行可能なサービスを自動的に判定する工程と、を含むことを特徴とするネットワーク自動初期化方法。

【請求項13】 前記ユーザおよびグループ情報を提供する工程は、前記デバイスが前記ネットワークに接続されたことを検出する工程と、

前記デバイスが前記ネットワークに接続されたことに応じて、前記デバイスに第1のユーザおよびグループリストを送信する工程と、

前記デバイスにおいて、前記第1のユーザおよびグループリストと前記デバイスに常駐している第2のユーザおよびグループリストとを比較する工程と、

前記デバイスにおいて、前記第1のユーザおよびグルー

プリストと前記第2のユーザおよびグループプリストとのいずれがより新しいものであるかを判定する工程と、前記デバイスからより新しいユーザおよびグループプリストを受信する工程と、前記より新しいユーザおよびグループプリストを反映させるために前記ユーザおよびグループ情報を更新する工程と、前記更新したユーザおよびグループ情報を前記ネットワーク全体に伝送する工程と、を含むことを特徴とする請求項12に記載のネットワーク自動初期化方法。

【請求項14】 前記第1のユーザおよびグループプリストと前記第2のユーザおよびグループプリストとのいずれがより新しいものであるかを判定する際に、タイムスタンプが使用されることを特徴とする請求項13に記載のネットワーク自動初期化方法。

【請求項15】 前記ユーザおよびグループ情報を更新する工程は、前記より新しいユーザおよびグループプリストをクリアテキストに記録する工程を含むことを特徴とする請求項13に記載のネットワーク自動初期化方法。

【請求項16】 前記ユーザおよびグループ情報を更新する工程は、前記ネットワーク全体に伝送する前に、前記ユーザおよびグループ情報を暗号化する工程を含むことを特徴とする請求項15に記載のネットワーク自動初期化方法。

【請求項17】 さらに、前記ネットワークアドレスおよび前記ネットワーク名を関連付けする工程と、前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、を含むことを特徴とする請求項12に記載のネットワーク自動初期化方法。

【請求項18】 前記ネットワーク名は、前記デバイスによって提示されるものであることを特徴とする請求項12に記載のネットワーク自動初期化方法。

【請求項19】 HTTP (HyperText Transfer Protocol) を使用して情報を交換することを特徴とする請求項12に記載のネットワーク自動初期化方法。

【請求項20】 SLP (Service Location Protocol) を使用して情報を交換することを特徴とする請求項12に記載のネットワーク自動初期化方法。

【請求項21】 第1のデバイスが接続されるネットワークであって、前記第1のデバイスは、第1のネットワークアドレスをリクエストし、前記ネットワークに接続されている第2のデバイスから前記第1のネットワークアドレスを受信し、前記第2のデバイスから前記第1のネットワークアドレスを受信できない場合に、ネットワークコンフィグレーションを提供し、前記第2のデバイスから前記第1のネットワークアドレ

スを受信した場合に、前記ネットワーク上におけるその優先順位を決定し、

前記優先順位が前記第2のデバイスの第2の優先順位より高い場合に、前記ネットワークコンフィグレーションを提供するように構成されていることを特徴とするネットワーク。

【請求項22】 前記第1のデバイスは、ネットワークに接続されるオフィス機器であることを特徴とする請求項21に記載のネットワーク。

【請求項23】 前記第1のデバイスは、さらに、第2のネットワークアドレスを自動的に割り当て、ネットワーク名を自動的に割り当て、前記第2のネットワークアドレスを前記ネットワーク名に自動的に関連付け、前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名を自動的にテーブルに記録するように構成されていることを特徴とする請求項21に記載のネットワーク。

【請求項24】 前記テーブルは、さらに、MAC (Media Access Control) アドレスと、前記ネットワーク名との競合を示すコードと、を含むことを特徴とする請求項23に記載のネットワーク。

【請求項25】 前記第1および第2のネットワークアドレスは、IP (Internet Protocol) アドレスを含むことを特徴とする請求項23に記載のネットワーク。

【請求項26】 第1のデバイスを含むネットワークであって、前記第1のデバイスは、前記ネットワーク上の第2のデバイスにアドレスを割り当て、前記ネットワーク上の前記第2のデバイスにネットワーク名を割り当て、前記ネットワーク全体にユーザおよびグループ情報を提供し、前記ネットワーク上の前記第2のデバイスで実行可能なサービスを判定するように構成されていることを特徴とするネットワーク。

【請求項27】 前記ユーザおよびグループ情報は、リストを含み、前記リストは、ユーザ名と、パスワードと、前記グループにアクセスすることが許可されているメンバーの第2のリストを有するグループ名と、タイムスタンプと、文字符号化コードと、を含むことを特徴とする請求項26に記載のネットワーク。

【請求項28】 前記パスワードは、クリアテキストに記録されることを特徴とする請求項27に記載のネットワーク。

【請求項29】 個々のサービスのリストを収集する工程と、

ネットワーククライアントからアクセス可能なマスターサービスリストを生成する工程と、

第1のネットワークデバイスのために、前記マスターサービスリストにアクセスして第2のネットワークデバイスが所望のサービスを用意しているか否かを判定する工程と、

を含むことを特徴とするサービス自動発見方法。

【請求項30】 さらに、クライアントをリソースロケータにプッシュし、新たなデバイスによって提供されるサービスを前記クライアントに通知する工程を含むことを特徴とする請求項29に記載のサービス自動発見方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、概して、ネットワークを自動的にコンフィグレーション (configuration; 構成) する方法および装置に関し、より詳細には、ネットワークに接続されるオフィス機器を含む動的なコンフィグレーションが可能なネットワークアーキテクチャ (dynamically configurable network architecture) に関する。

【0002】

【従来の技術】 一般に、ネットワークで接続されている環境においてあるデバイスを動作させる前に、そのデバイスについて適切なコンフィグレーションを行っておく必要がある。各デバイスに対して要求される特定のネットワークコンフィグレーションは、ネットワークトポロジーやデバイスの機能のようなファクタに応じて変化する可能性がある。TCP/IP (Transmission Control Protocol/Internet Protocol) ネットワーク上において、各デバイスまたはホストにはIPアドレスとして知られている一意的な名前が割り当てられる。

【0003】 IPアドレスは、通常、ピリオドで分離された数字4個で構成された32ビットの数値アドレスの形態をとるものであるが、特定のネットワークトポロジーに応じて異なる場合もある。なお、IPアドレスのフォーマットに関するより詳細な情報については、Request For Comments (RFC) 1700, "Assigned Numbers", October 1994から得ることができる。

【0004】 ところで、TCP/IPネットワークを介してホストとの通信を確立することに先立ち、通信を開始する者は、電話番号に良く似た宛先ホストのIPアドレスが電話をかける際に使用されるかを調べる。その者は常に受信側のIPアドレスを知っているとは限らず、不幸にもそのIPアドレスを確かめるための単純な方法も存在していない。しかしながら、簡略的なネットワーク通信を考慮に入れたドメイン名 (domain name) のようなメカニズムが幸いにも開発されている。

【0005】 ドメイン名は、ユーザがリモートホストと通信することを単純化する手段として導入されたものである。ドメイン名に関する背景情報および仕様については、RFC 1034, "Domain Names - Concepts and Facilities", November 1987および対となるRFC 1035, "Domain Names - Implementation and Specification", November 1987で得ることができる。その最も単純なフォームにおいて、ドメイン名は一以上のユニークな数字のIPアドレスからなる人間が判読可能なテキスト表現以外の何物でもない。ドメイン名を使用することにより、ユーザはホストと通信を行うために多数の厄介なIPアドレスを記憶しておく必要はなく、むしろ該当するホストのドメイン名を覚える必要があるだけである。

【0006】 さらに、大部分のドメイン名はそれらの対応するホスト名のいくつかのバリエーションを反映したものであり、それゆえユーザのための簡略記憶記号としての働きを持つ。しかしながら、インターネットはドメイン名ではなく、IPアドレッシングに基づくものであるため、ネットワークに接続されるデバイスは通信の開始前に全てのホストのドメイン名をホストの対応するIPアドレスに置き換える必要がある。この置換プロセスはDNS (domain name service) として知られているものによって容易化が図られている。

【0007】 図10は、従来技術に基づくDNSの構成を示す図である。図10において、クライアント100はホスト115のドメイン名102を送信し、クライアント100がネットワーク101を介してDNSサーバ120との通信を要望する。DNSサーバ120は、そのデータベース118においてルックアップ機能を実行し、対応するIPアドレス103を検索してクライアント100に返送する。そして、クライアント100は、ホストの対応するIPアドレス103を用いてホスト115との通信を確立することができる。

【0008】 DNSサーバによって一つのホストドメイン名が複数のIPアドレスにリンクされることは珍しくはない。一以上のホストのIPアドレスが変更され、またはネットワークから削除された場合、対応するDNSのエントリを変更し、またはDNSデータベースから削除する必要がある。DNSが有する一つの限界は、従来よりそのようなアドレスの変更を自動的にアップデートすることができないということである。

【0009】 現在、DNSのアップデートはマニュアルで実行されることが一般的であり、その作業は多くの場合時間がかかり、細部まで正確な精度が必要とされる。しかしながら、そのようなマニュアルアップデートはDNSデータベースだけに限定されるものではない。すなわち、IPアドレスのような基本的なコンフィグレーション情報も、従来よりマニュアルでホストに割り当てられている。

【0010】 マニュアルによるIPアドレスの割り当て

は、ほとんどの場合ネットワーク管理者のような経験豊かな者によって行われている。ネットワーク管理者は、ネットワーク管理者によって利用可能であることが知られているアドレスのブロックから選択されたIPアドレスを各ホストに割り当てる。ホストのコンフィグレーションを行う際にネットワーク管理者がIPアドレスをミスタイプするようなことがあると、ホストは正しく機能しない可能性がある。同様に、ネットワーク管理者が予め割り当てられているIPアドレスをホストに割り当てたりすると、IPアドレスの競合による通信エラーが発生する場合がある。

【0011】また、IPアドレス以外のさらなるTCP/IPコンフィグレーション情報もしくはマニュアルで入力される。多くの場合、TCP/IPコンフィグレーションプロセスは、管理者に対して各ホストを個別に訪れて適切な情報を入力するように要求する。また、ホストのコンフィグレーションがその後変更される毎に、管理者はホストを訪れてアップデートを行わなければならない。大規模なネットワークにおいてこのようなやり方でコンフィグレーションをマニュアルでアップデートすると、非常に時間がかかることになる。

【0012】動的なIPアドレスアロケーションは、マニュアルによるホストコンフィグレーションで引き起こされるいくつかの問題の解決を試みたものである。動的なIPアドレスアロケーションの異なるインプリメンテーションが時間の経過と共に提案されてきてはいるが、今日使用されている一つの一般的なプロトコルはDHCP (Dynamic Host Configuration Protocol) である。DHCPのさらなる情報については、RFC 2131, "Dynamic Host Configuration Protocol", March 1997で得ることができる。DHCPはブートストラッププロトコル (Bootstrap Protocol: BOOTP) に基づくものであるが、DHCPは再使用可能なネットワークアドレスおよび追加のコンフィグレーションオプションを自動的に割り当てる機能を追加するものである。

【0013】BOOTPに関する詳細な情報については、RFC 951, "Bootstrap Protocol (BOOTP)", September 1985から得ることができる。DHCPは、ブート時に、TCP/IPネットワーク上においてコンフィグレーション情報をホストに渡すためのフレームワークを提供するものである。DHCPにより、ネットワーク管理者が各ホストを個別に訪れてホストのコンフィグレーションを行ったり、変更したりする必要をなくすることができる。

【0014】コンフィグレーションは、ホストIPアドレスや、ドメインネームサーバ、デフォルトゲートウェイおよびサブネットマスクの定義のような他のTCP/IPオプション設定を含む場合がある。いくつかのDHCPサーバのインプリメンテーションはオプションセットの使用を考慮しており、その結果、ネットワーク管理

者が共通の設定を特定のオプションに割り当てることを可能にする。管理者がオプションセットの変更を行う場合、そのオプションセットを使用しているクライアントのコンフィグレーションはアップデート情報を受信することになる。このように、中央管理がより簡単なものとなる。

【0015】図10は、従来技術に基づくDHCPのコンフィグレーションを示す図である。図10において、そのブートストラップルーチンを開始することに応じ、DHCPクライアント100はDHCPクライアント100に設定を返信することができるDHCPサーバ110または111を捜すDHCPDISCOVER BROADCAST105をネットワーク101全体に送信する。ネットワーク101上の使用可能なDHCPサーバ110および111の両方は、DHCPクライアント100からDHCPDISCOVER BROADCAST105を受信し、そのような特定のクライアント100に対してコンフィグレーション情報を提供可能であるか否かを判定する。

【0016】DHCPサーバ110および111がリクエストしているクライアント100に関するコンフィグレーションを有している場合、DHCPサーバ110および111はネットワーク101を介してDHCP OFFER106をDHCPクライアント100に送信する。DHCPクライアント100は、DHCPサーバ110および111から受信した全てのDHCP OFFER106を分析し、DHCPサーバ110および111のいずれか一つを選択し、選択したDHCPサーバ、たとえばDHCPサーバ110にネットワーク101を介してDHCP REQUEST107を送り返す。DHCPサーバ110は、DHCP ACKNOWLEDGE108をDHCPクライアント100に対して発行し、IPアドレスを確保し、続いてネットワーク101を介してDHCPクライアント100に対してコンフィグレーション情報を配信する。

【0017】DNSと共にDHCPを利用しているネットワークの持つ現在の問題の一つとして、DNSおよびDHCPの二つのシステム間における通信の欠如が挙げられる。IPアドレスが動的にホストに割り当てられる毎に、対応するドメイン名も割り当てられる場合がある。ホストのIPアドレスがたびたび変化するネットワークにおいて、そのドメイン名も同様に変化することになる。そのようなアドレス/ドメイン名の割り当てに関係するランダム性のため、そのような割り当てがDNSにも反映されることが重要である。

【0018】しかしながら、DNSアップデートが多くなるとマニュアルで完了されるため、DNSが利用可能な最も新しいホストアドレス/ドメイン名情報を反映するようになる可能性は低い。DNSが最も新しいアドレス/ドメイン名の割り当てで最新の状態に保たれていな

い場合、ホスト間の通信はますます難しくなることが考えられる。たとえDNSデータベースが利用可能な最も新しいネットワークアドレス/ドメイン名情報で最新の状態に保たれたとしても、依然として一つの固定されたドメイン名でひとつのホストを都合良く特定することはできる。一つの固定されたドメイン名により、ホストの動的に割り当てられたIPアドレスが何であるかに関係なく、ドメイン名を介してあらゆる特定のホストと常に連絡することが可能である。

【0019】したがって、動的にIPアドレスをホストに割り当て、一方、静的に単一のドメイン名をそのホストに割り当てることが可能なシステムを有するようにすることが望ましい。そのようなシステムは、システムに対する人間の介入を最小限にして必要なDNSアップデートを自動的に実行し、それによって通信エラーを最小限に抑える。

【0020】

【発明が解決しようとする課題】デバイスがコンフィグレーションされてネットワークに接続されると、ネットワーク管理者はユーザおよびグループ情報をアップデートすることや、そのデバイスに対するアクセス権を割り当てることに関して責任を持つことが一般的である。ネットワークのサイズや接続されたデバイスの数が増大するにつれて、ユーザおよびグループ情報をアップデートするプロセスやアクセス権を与えるプロセスが膨大なタスクになる可能性がある。

【0021】大規模なオフィス環境において、多くの場合、ユーザおよびグループ情報のアップデートはネットワークの機能にとって重大なものとは考えられておらず、従ってより緊急的なシステムの問題のような他のものより低い優先順位が割り当てられている。指定されたネットワーク管理者さえ存在しない小規模なオフィス環境においては、ネットワークコンフィグレーションおよびネットワーク管理の実行は訓練されていない者に任せられている。そのようなやり方は生産性に影響を及ぼすだけでなく、ネットワークの機能を危うくする場合もある。

【0022】したがって、簡単、快適、および家電品のような自動コンフィグレーション機能 (appliance-like automatic configuration features) をユーザに提供するネットワークデバイスを有するようにすることが望ましい。指定の管理者を欠くネットワーク環境に配置される場合、そのようなデバイスはネットワークオペレーションに対して自動的にそれ自体をコンフィグレーションすることが可能なものであり、同時に、管理されたネットワーク環境に配置される場合、そのデバイスは先にネットワークに接続された機器との相互接続性を提供するものである。

【0023】

【課題を解決するための手段】ネットワーク上の第1の

デバイスを初期化する方法および装置が開示される。最初に、第1のデバイスがネットワークに接続されると、第2のデバイスからのコンフィグレーション情報がリクエストされる。そして、初期化プロセスがある期間にわたって遅延させられる。つぎに、初期化プロセスを遅延させる期間内に第2のデバイスからコンフィグレーション情報に対する応答が受信されない場合、コンフィグレーションサービスがネットワークに提供される。第1のデバイスが第2のデバイスより高い優先順位を有している場合、コンフィグレーションサービスがネットワークに提供される。ネットワークは、さらなるデバイスがネットワークに接続されることを検出するために連続的にモニタされる。

【0024】すなわち、請求項1のデバイス初期化方法は、ネットワーク上の第1のデバイスを自動的に初期化するデバイス初期化方法であって、前記ネットワークに前記第1のデバイスを接続すると、第2のデバイスからのコンフィグレーション情報をリクエストする工程と、コンフィグレーション情報を取得できないと決定する前に、任意の期間遅延させる工程と、前記期間内に前記第2のデバイスから前記コンフィグレーション情報のリクエストに対する応答を受信しなかった場合に、前記ネットワークにコンフィグレーションサービスを提供する工程と、前記第1のデバイスが前記第2のデバイスより高い優先順位を有している場合に、前記ネットワークに前記コンフィグレーションサービスを提供する工程と、さらなるデバイスが前記ネットワークに接続されたことを検出するために前記ネットワークを連続的にモニタする工程と、を含むものである。

【0025】また、請求項2のデバイス初期化方法は、請求項1に記載のデバイス初期化方法において、前記コンフィグレーションサービスを提供する工程が、第1のネットワークアドレスを自動的に決定する工程と、第2のネットワークアドレスを自動的に割り当てる工程と、ネットワーク名を自動的に割り当てる工程と、前記第1のネットワークアドレス、前記第2のネットワークアドレスおよび前記ネットワーク名を自動的に関連付ける工程と、前記関連付けられた第1のネットワークアドレス、前記関連付けられた第2のネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、を含むものである。

【0026】また、請求項3のデバイス初期化方法は、請求項2に記載のデバイス初期化方法において、前記第1のネットワークアドレスが、MAC (media access control) アドレスを含むものである。

【0027】また、請求項4のデバイス初期化方法は、請求項2に記載のデバイス初期化方法において、前記第2のネットワークアドレスが、IP (Internet Protocol) アドレスを含むものである。

【0028】また、請求項5のデバイス初期化方法は、



請求項2に記載のデバイス初期化方法において、前記ネットワーク名を割り当てる工程が、ネットワーク名の競合を検出する工程と、前記ネットワーク名の競合を解決する工程と、前記ネットワーク名の競合を示すコードを前記テーブルに記録する工程と、を含むものである。

【0029】また、請求項6のデバイス初期化方法は、請求項2に記載のデバイス初期化方法において、前記ネットワーク名が、前記第1のデバイスによって提示されるものである。

【0030】また、請求項7のデバイス初期化方法は、請求項1に記載のデバイス初期化方法において、前記期間が、競合状態を防ぐために異なるものである。

【0031】また、請求項8のネットワーク情報の自動割り当て方法は、ネットワークアドレスをデバイスに割り当てる工程と、ネットワーク名を前記デバイスに割り当てる工程と、前記ネットワーク名を前記ネットワークアドレスに関連付ける工程と、前記割り当てられたネットワークアドレスから独立している前記割り当てられたネットワーク名でユーザが前記デバイスを参照することができるように、前記関連付けられたネットワーク名および前記関連付けられたネットワークアドレスをテーブルに記録する工程と、を含むものである。

【0032】また、請求項9のネットワーク情報の自動割り当て方法は、請求項8に記載のネットワーク情報の自動割り当て方法において、前記ネットワーク名を割り当てる工程が、前記ネットワーク名が既に使用中の場合、ネットワーク名の競合を解決する工程を含むものである。

【0033】また、請求項10のネットワーク情報の自動割り当て方法は、請求項9に記載のネットワーク情報の自動割り当て方法において、前記ネットワーク名が、前記デバイスによって提示されるものである。

【0034】また、請求項11のネットワーク情報の自動割り当て方法は、請求項8に記載のネットワーク情報の自動割り当て方法において、前記ネットワークアドレスが、DHCP (Dynamic Host Configuration Protocol) を使用して割り当てられるものである。

【0035】また、請求項12のネットワーク自動初期化方法は、ネットワークを自動的に初期化するためのネットワーク自動初期化方法であって、前記ネットワーク上のデバイスにアドレスを自動的に割り当てる工程と、前記ネットワーク上の前記デバイスにネットワーク名を自動的に割り当てる工程と、前記ネットワーク全体にユーザおよびグループ情報を自動的に提供する工程と、前記ネットワーク上の前記デバイスが実行可能なサービスを自動的に判定する工程と、を含むものである。

【0036】また、請求項13のネットワーク自動初期化方法は、請求項12に記載のネットワーク自動初期化方法において、前記ユーザおよびグループ情報を提供する工程は、前記デバイスが前記ネットワークに接続され

たことを検出する工程と、前記デバイスが前記ネットワークに接続されたことに応じて、前記デバイスに第1のユーザおよびグループリストを送信する工程と、前記デバイスにおいて、前記第1のユーザおよびグループリストと前記デバイスに常駐している第2のユーザおよびグループリストとを比較する工程と、前記デバイスにおいて、前記第1のユーザおよびグループリストと前記第2のユーザおよびグループリストとのいずれがより新しいものであるかを判定する工程と、前記デバイスからより新しいユーザおよびグループリストを受信する工程と、前記より新しいユーザおよびグループリストを反映させるために前記ユーザおよびグループ情報を更新する工程と、前記更新したユーザおよびグループ情報を前記ネットワーク全体に伝送する工程と、を含むものである。

【0037】また、請求項14のネットワーク自動初期化方法は、請求項13に記載のネットワーク自動初期化方法において、前記第1のユーザおよびグループリストと前記第2のユーザおよびグループリストとのいずれがより新しいものであるかを判定する際に、タイムスタンプが使用されるものである。

【0038】また、請求項15のネットワーク自動初期化方法は、請求項13に記載のネットワーク自動初期化方法において、前記ユーザおよびグループ情報を更新する工程が、前記より新しいユーザおよびグループリストをクリアテキストに記録する工程を含むものである。

【0039】また、請求項16のネットワーク自動初期化方法は、請求項15に記載のネットワーク自動初期化方法において、前記ユーザおよびグループ情報を更新する工程が、前記ネットワーク全体に伝送する前に、前記ユーザおよびグループ情報を暗号化する工程を含むものである。

【0040】また、請求項17のネットワーク自動初期化方法は、請求項12に記載のネットワーク自動初期化方法において、さらに、前記ネットワークアドレスおよび前記ネットワーク名を関連付けする工程と、前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、を含むものである。

【0041】また、請求項18のネットワーク自動初期化方法は、請求項12に記載のネットワーク自動初期化方法において、前記ネットワーク名が、前記デバイスによって提示されるものである。

【0042】また、請求項19のネットワーク自動初期化方法は、請求項12に記載のネットワーク自動初期化方法において、HTTP (HyperText Transfer Protocol) を使用して情報を交換するものである。

【0043】また、請求項20のネットワーク自動初期化方法は、請求項12に記載のネットワーク自動初期化方法において、SLP (Service Location Protocol) を使用して情報を交換するものである。

【0044】また、請求項21のネットワークは、第1のデバイスが接続されるネットワークであって、前記第1のデバイスが、第1のネットワークアドレスをリクエストし、前記ネットワークに接続されている第2のデバイスから前記第1のネットワークアドレスを受信し、前記第2のデバイスから前記第1のネットワークアドレスを受信できない場合に、ネットワークコンフィグレーションを提供し、前記第2のデバイスから前記第1のネットワークアドレスを受信した場合に、前記ネットワーク上におけるその優先順位を決定し、前記優先順位が前記第2のデバイスの第2の優先順位より高い場合に、前記ネットワークコンフィグレーションを提供するように構成されているものである。

【0045】また、請求項22のネットワークは、請求項21に記載のネットワークにおいて、前記第1のデバイスが、ネットワークに接続されるオフィス機器であるものである。

【0046】また、請求項23のネットワークは、請求項21に記載のネットワークにおいて、前記第1のデバイスが、さらに、第2のネットワークアドレスを自動的に割り当て、ネットワーク名を自動的に割り当て、前記第2のネットワークアドレスを前記ネットワーク名に自動的に関連付け、前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名を自動的にテーブルに記録するように構成されているものである。

【0047】また、請求項24のネットワークは、請求項23に記載のネットワークにおいて、前記テーブルが、さらに、MAC (Media Access Control) アドレスと、前記ネットワーク名との競合を示すコードと、を含むものである。

【0048】また、請求項25のネットワークは、請求項23に記載のネットワークにおいて、前記第1および第2のネットワークアドレスが、IP (Internet Protocol) アドレスを含むものである。

【0049】また、請求項26のネットワークは、第1のデバイスを含むネットワークであって、前記第1のデバイスが、前記ネットワーク上の第2のデバイスにアドレスを割り当て、前記ネットワーク上の前記第2のデバイスにネットワーク名を割り当て、前記ネットワーク全体にユーザおよびグループ情報を提供し、前記ネットワーク上の前記第2のデバイスで実行可能なサービスを判定するように構成されているものである。

【0050】また、請求項27のネットワークは、請求項26に記載のネットワークにおいて、前記ユーザおよびグループ情報がリストを含み、前記リストは、ユーザ名と、パスワードと、前記グループにアクセスすることが許可されているメンバーの第2のリストを有するグループ名と、タイムスタンプと、文字符号化コードと、を含むものである。

【0051】また、請求項28のネットワークは、請求項27に記載のネットワークにおいて、前記パスワードが、クリアテキストに記録されるものである。

【0052】また、請求項29のサービス自動発見方法は、個々のサービスのリストを収集する工程と、ネットワーククライアントからアクセス可能なマスターサービスリストを生成する工程と、第1のネットワークデバイスのために、前記マスターサービスリストにアクセスして第2のネットワークデバイスが所望のサービスを用意しているか否かを判定する工程と、を含むものである。

【0053】さらに、請求項30のサービス自動発見方法は、請求項29に記載のサービス自動発見方法において、さらに、クライアントをリソースロケータにプッシュし、新たなデバイスによって提供されるサービスを前記クライアントに通知する工程を含むものである。

【0054】

【発明の実施の形態】以下、本発明に係るネットワークに接続されるオフィス機器 (office appliance; OA) のアーキテクチャについて説明する。以下の説明において、特定の構成要素、コンフィグレーション、接続等のような多数の特定の実施の形態を明らかにし、本発明を完全に理解できるようにする。ただし、当業者にとって明らかなように、本発明を実施するためにこれらの特定の実施の形態を適用する必要があるわけではない。他の例において、公知の構成要素または公知の方法については、本発明が不明瞭なものとならないようにするためにあえて詳細な説明を省略する。

【0055】後述する実施の形態における若干の部分は、アルゴリズム、およびコンピュータメモリ内のデータビットに基づくオペレーションの記号表現の観点から表現される。これらのアルゴリズムの説明および表現は、データ処理技術の当業者らによって、その技術の他の当業者らに彼/彼女らの仕事の要旨を最も効果的に伝えるために使用される手段である。アルゴリズムは、所望の結果に導く首尾一貫した複数のステップのシーケンスであるところここで一般に理解される。

【0056】各ステップは、物理量の物理的操作を必要とするものである。必ずしも必要とされるわけではないが、これらの量は記憶され、伝送され、組み合わせられ、比較され、さらには処理されることが可能な電気信号または磁気信号の形態をとることが通常である。これらの信号をビット、値、要素、シンボル、キャラクタ、ターム、数字等と呼ぶことは、主として一般的な用法という理由からときどき便利であることがわかっている。

【0057】しかしながら、これらおよび類似のタームの全ては、該当する物理量と関連付けられることになること、およびこれらの量に適用される単なる便利なラベルであるということに留意すべきである。後述する説明から明らかなように、特に言及しない限り、本発明全体において「処理 (processing)」, 「コンピューティン

グ (computing)」、 「計算 (calculating)」、 「判定 (determining)」、 「表示 (displaying)」 等のようなタームを利用した説明は、コンピュータシステムまたは類似の電子計算機のアクション (行為) および処理に言及するものであると理解される。

【0058】すなわち、コンピュータシステム等のアクション (行為) および処理は、コンピュータシステムのレジスタおよびメモリ内において物理 (電子) 量として表現されたデータを、コンピュータシステムのメモリもしくはレジスタまたは他のそのような情報ストレージデバイス、送信デバイスもしくは表示デバイス内において物理量として同様に表現された他のデータに処理すると共に変換するというようなものである。

【0059】また、本発明は、ここで説明するオペレーションを実行する装置に関するものでもある。この装置は、要求される目的のために特別に構成したものであっても良いし、コンピュータに格納されているコンピュータプログラムによって選択的に起動されまたは再構成される汎用コンピュータで構成したものであっても良い。そのようなコンピュータプログラムはつぎのものに限定されるわけではないが、フロッピーディスク・光ディスク・CD-ROMおよび光磁気ディスクのような任意の種類のディスク、リードオンリーメモリ (ROM)、ランダムアクセスメモリ (RAM)、EPROM、EEPROM、磁気もしくは光カード、または電子的な命令を格納するのに適したあらゆる種類の媒体を含むコンピュータ読み取り可能な記憶媒体に格納しておくことが可能であり、それらはコンピュータのシステムバスに任意の方法 (たとえば有線または無線) で接続される。

【0060】ここで提示されるアルゴリズムおよび表示は、いかなる特定のコンピュータまたは他の装置と本質的に関係するものではない。様々な汎用マシンがここで教示に基づくプログラムと共に使用される場合があり、または必要とされる処理を実行するためにより専門化された装置を構成することが便利であることがわかる場合もある。これらの装置の様々な必須の構成は以下の説明に見出されることになる。さらに、本発明は、いかなる特定のプログラム言語に関連して開示されるものではない。すなわち、ここに記述される本発明の教示を実現するために様々なプログラム言語が使用可能であることが理解されることになるであろう。

【0061】一以上の処理ユニットまたはデバイス (たとえばCPU)、コンピュータシステムまたは専用の装置において実行されるソフトウェアによってオペレーションの全てまたは一部が実行される場合があるが、これらのオペレーションの一部または全ては、デジタル論理回路および/もしくはデジタル回路、集積回路 (たとえばASIC) または他の半導体回路基板で実行される場合もある。

【0062】【概要】OAのアーキテクチャは、ネット

ワーク管理者を欠くオフィスにおいてコンフィグレーションまたはセットアップを必要とすることなく、ネットワークに機器を加えることを可能にする。同時に、OAのアーキテクチャは、先に存在しているネットワークデバイスとの競合を生じさせることなく、標準的な管理されたネットワークに機器を容易に加えることを可能にする。

【0063】さらに、複数のOAはネットワーク環境において密接に協力して動作し、ネットワークに接続されると情報を自動的に検出して互いに共有することができる。ネットワークに接続されるオフィス機器 (OA) の若干の例としては、つぎのようなデバイスに限定されるわけではないが、ファクシミリ装置、複写機、プリンタ、パーソナルコンピュータ、スキャナ、電子タイプライタ、データバックアップシステム、制御ユニット等のようなデバイスがある。

【0064】OAのアーキテクチャは、TCP/IPネットワークのようなネットワーク上のデバイスを自動的にコンフィグレーションするためのメカニズムを提供する。ここで開示される特定のコンフィグレーション方法は、ネットワークアドレスアロケーション (network address allocation)、DNSデータベースポピュレーション (DNS database population)、ネットワークサービスディスカバリ (network service discovery)、およびユーザアイデンティティシェアリング (user identity sharing) を含む。

【0065】これらのアルゴリズムに従う各デバイスは、それらがネットワーク上に存在していない場合に自動的にDHCPサービスおよびDNSサービスを開始し、そのようなサービスがネットワーク上に既に存在している場合にそれを行うことを停止する。DHCPサービスおよびDNSサービスの両方は、人間の介在なしに (自動的に) 同一ネットワーク上のネットワークデバイスに名前およびアドレスを与えるために協力して機能する。加えて、ユーザおよびグループ情報と同様に、サービス情報を安全に共有するHTTP (hypertext transfer protocol) ベースの方法も定義される。

【0066】開示されるアーキテクチャおよびシステムは、特定のメカニズムを使用してネットワークをコンフィグレーションする方法で従来のものとは異なる。そのようなメカニズムの一つは、ネットワーク上にDNSサービスおよびDHCPサービスの存在していることを検出する手だてとなるものであり、一方、別のメカニズムは、そのようなサービスが検出された場合にデバイスの応答を制御するものである。

【0067】DHCPサービスおよびDNSサービスがネットワーク上で検出された場合、OAデバイスはクライアントとして起動し、サービスによって提供されるあらゆるコンフィグレーション情報を受け取ることができる。一方、OAデバイスがDHCPサービスおよびDN

Sサービスを検出しなかった場合、そのOAデバイスはサーバとして起動し、それらのサービスをネットワークに提供することができる。OAのアーキテクチャは、状態変数、タイミングおよび通信プロトコルの組み合わせを使用してこれらのタスクを実行する。

【0068】サービスディスカバリは、開示された自動ネットワークコンフィグレーション内で実行されるものである。任意に指定されたサービスデバイスは、ユニークなプロトコルを利用してネットワーク上の複数のOAデバイスから個々のサービスリストを収集する。その際に、サービスデバイスは、ネットワーク上の全てのOAデバイスがアクセス可能なマスタサービスリストを生成する。このように、各OAデバイスは、ネットワーク上のその他全てのOAデバイスが提供する各サービスを識別することができる。

【0069】ユーザおよびグループ情報は、自動的にコンフィグレーションされたネットワーク全体で共有される。ユーザおよびグループ情報は、どのユーザがあるOAデバイスにアクセスすることが許可されているのかを、許可されているアクセスレベルと共に表す情報である。OAアーキテクチャは、HTTPプロトコルに関連したユニークなプロトコルを利用して、複数のOAデバイス間でユーザおよびグループ情報の受け渡しを行う。OAデバイスが自動的にコンフィグレーションされたネットワークに接続される場合、ユーザおよびグループ情報はそのOAデバイスに渡される。

【0070】OAデバイスは、渡されたユーザおよびグループ情報が、既に有している既存のユーザおよびグループ情報より新しいか古いかを検出することができる。OAデバイスが、上記のようにして受け取ったユーザおよびグループ情報の送信元のデバイスにより新しいユーザおよびグループ情報を返送し、そのユーザおよびグループ情報がネットワーク全体に伝搬されるようにすることを可能にするさらなるメカニズムも提供される。

【0071】OAのアーキテクチャは、ここで開示される自動的にコンフィグレーションされるネットワークにおけるネットワーク名の競合を解決するためのさらなるメカニズムを提供する。各OAデバイスが、割り当てられるそれらの自身のネットワーク名を選択することができるため、2以上のOAが同一名を選択する可能性がある。2以上のOAが同一名を選択するような場合、OAデバイスは、新規な競合解決プロセスを使用して、選択されたネットワーク名をユニークであるが一貫したものにすることで競合を解決する。

【0072】以下のセクションにおいて、OAのアーキテクチャにおいて利用される特定のメカニズムおよびプロトコルについてさらに詳細に説明する。

【0073】〔クライアントOAのコンフィグレーション〕図1は、OAのアーキテクチャの一実施の形態を示す図である。図1において、クライアントOA200は

ネットワーク201に接続されている。ネットワーク201は、インターネット、イントラネットまたは複数のデバイスが情報を共有可能なあらゆる種類の相互接続されたデータバス等、いかなるものであっても良い。ホスト202は、非OAサーバ210と同様に、ネットワーク201に接続されることが可能な非OAネットワークデバイスである。非OAサーバ210は、DHCPまたは等価のサービスをネットワーク201に提供可能なものであっても良いし、提供することが不可能なものであっても良い。なお、ネットワーク201に接続可能なホスト202および非OAサーバ210の数は任意である。

【0074】図2は、クライアントOAのネットワークコンフィグレーションの一実施の形態を示すフローチャートである。図2において、そのブートストラップシーケンスを開始すると、クライアントOA200は、ネットワーク201上において正しく機能するために必要とされる必要なコンフィグレーション情報を取得しようとする。DHCPプロトコルを使用することにより、クライアントOA200は、時間間隔D毎にネットワーク201全体にDHCPDISCOVERをブロードキャスト(broadcast)する(S322)。この処理はクライアントOA200がDHCP OFFERを受信するか(S326)、またはDHCP応答に割り当てられた予め設定された時間が経過(満了)するまで(S330)実行される。

【0075】ステップS324における特定の遅延時間間隔Dは、連続するDHCPDISCOVERがステップS322でブロードキャストされる間の時間の基準である。遅延時間間隔Dは、ステップS326でクライアントOA200がDHCP OFFERを待つ予め設定された時間と同様に変更することが可能である。非OAサーバ210がDHCPサービスをネットワーク201に提供できるように構成されている場合、非OAサーバ210はクライアントOA200に対してDHCP OFFERで応答し、必要とされるコンフィグレーション情報をクライアントOA200に提示する。どのような理由にせよ、クライアントOA200が非OAサーバ210で提示されたコンフィグレーション情報を承認しない場合、クライアントOA200はステップS327でDHCPREQUESTを送信することなく、ステップS332でDHCPDECLINEを非OAサーバ210に発行する。

【0076】クライアントOA200は、ステップS326で別のDHCP OFFERが受信されるか、ステップS330でDHCP応答のために割り当てられた予め設定された時間が経過するまで、ステップS322においてDHCPDISCOVERのブロードキャストを続ける。一方、クライアントOA200が非OAサーバ210によって提示されたコンフィグレーション情報を承

認する場合、クライアントOA200は、ステップS327でDHCPREQUESTを非OAサーバ210に送信することによって提示されたコンフィグレーション情報をリクエストする。

【0077】クライアントOA200に提示されたコンフィグレーション情報が未だ有効かつ利用可能な場合、非OAサーバ210はステップS328で受信されるDHCPACKNOWLEDGEをクライアントOA200に伝送し、クライアントOA200用のIPアドレスを確保し、そして同意されたコンフィグレーション情報をネットワーク201を介してクライアントOA200に伝送する。このように、クライアントOA200はステップS329で無事にブートを継続する。ただし、たとえば同一のアドレスがいくつかのホストに提示され、そしてそれらのホストの一つが受け入れた場合、コンフィグレーション情報は有効かつ利用可能ではない。この点で、他の提示ももはや有効ではない。

【0078】どのような理由にせよ、ステップS328においてDHCPACKNOWLEDGEがクライアントOA200で受信されなかった場合、クライアントOA200は、ステップS326で別のDHCPOFFERが受信されるか、またはステップS330でDHCP応答のために割り当てられた予め設定された時間が経過するまで、ステップS322においてDHCPDISCOVERのブロードキャストを続行する。

【0079】一実施の形態において、非OAサーバ210はDHCPまたは等価なサービスをネットワーク201に提供できるように構成されていないものとする。この場合、クライアントOA200は、ネットワーク201全体にDHCPDISCOVERをブロードキャストすると共に、ネットワーク201全体につぎのDHCPDISCOVERをブロードキャストする前に、ステップS324で特定の時間間隔Dだけ遅延させる。DHCP応答のために割り当てられた予め設定された時間が経過すると、最終的にステップS331においてエラー状態が引き起こされる。

【0080】エラー状態が引き起こされると、ユーザまたは管理者は、自動コンフィグレーションが可能でないことについて音声または視覚的な通知で警告される。視覚的なエラー通知は、CRT (Cathode Ray Tube) を含む任意のディスプレイデバイス上に表示可能なものである。なお、ディスプレイデバイスはネットワークに接続されていても良いし、接続されていなくても良い。代替的に、エラー状態の通知を後に管理者が検索して検査できるようにするため、エラーログという形で磁気媒体上にアーカイブすることにしても良い。

【0081】一実施の形態においては、少なくとも二つのOAサーバ210がネットワーク201に接続されており、それらOAサーバ210の少なくとも二つがDHCPサービスをネットワーク201に提供するように構

成されている。DHCPプロトコルを使用することにより、クライアントOA200は、クライアントOA200がステップS326においてDHCPOFFERを受信するか、またはステップS330においてDHCP応答用に割り当てられた予め設定された時間が経過するまで、時間間隔D毎にステップS322においてネットワーク201全体にDHCPDISCOVERをブロードキャストする。DHCPサービスを提供するように構成されていると共に、クライアントOA200にコンフィグレーション情報を提供することができる非OAサーバ210は、クライアントOA200に対してDHCPOFFERで応答する。

【0082】クライアントOA200がステップS326で複数の非OAサーバ210から複数のDHCPOFFERを受信した場合、クライアントOA200はコンフィグレーションを受け入れるか否かを判定し、受け入れると判定した場合、受信した複数のコンフィグレーションのどの一つを受け入れるかを判定する。クライアントOA200が全てのコンフィグレーションの拒否を選択する場合、クライアントOA200は、ステップS332において、コンフィグレーションを提示した非OAサーバに対してDHCPDECLINEを発行する。クライアントOA200は、より条件に合ったDHCPOFFERがステップS326で受信されるか、またはステップS330においてDHCP応答のために割り当てられた予め設定された時間が経過するまで、ステップS322でDHCPDISCOVERのブロードキャストを継続する。

【0083】一方、クライアントOA200が複数の非OAサーバ210の一つによって提示されたコンフィグレーションの受け入れを選択した場合、クライアントOA200はステップS327において該当する非OAサーバ210、即ち条件にあったDHCPOFFERを提示した非OAサーバ210に対してDHCPREQUESTを発行する。また、クライアントOA200は、ステップS332において、受け入れることができないDHCPOFFERを提示した全ての非OAサーバ210に対してDHCPDECLINEを発行する。

【0084】なお、複数のクライアントOA200をネットワーク201に接続することにしても良い。複数のクライアントOAが一つのネットワークに接続されるこのような例において、特定のクライアントOAのコンフィグレーションプロセスは、単一のクライアントOAについて説明したコンフィグレーションプロセスと同一であっても良い。

【0085】DHCPプロトコルに関連してコンフィグレーションについて説明したが、類似の機能を有した他のプロトコルを使用しても良いことはいうまでもない。

【0086】[OAサーバの自己識別] 一実施の形態において、クライアントOAデバイスを含むネットワーク

は、2以上のOAサーバを含んでいる。これらのOAサーバは、DNS、DHCP、サービスディスカバリ (service discovery)、およびユーザマネジメント機能のようなコンフィグレーションサービスをクライアントOAを含むネットワークに提供し、そして、任意の与えられた時間にいずれのOAサーバが残りのOAサーバより高い優先順位が与えられるかを管理することができる。最も高い優先順位を有するOAサーバはマスタサーバとして指定されると共に、OAのネットワークに大容量のコンフィグレーションサービスを供給する。

【0087】OAサーバは、あるデバイスがネットワークにコンフィグレーションサービスを現在提供しているか否か、またはコンフィグレーションサービスがネットワークで必要とされているか否かを判定することができる。あるOAサーバがネットワークに接続される際、そのOAサーバはネットワーク全体にDHCPDISCOVERをブロードキャストする。OAサーバがDHCPDISCOVERに対するDHCPOFFERを受信しなかった場合、他のいかなるデバイスもネットワークにコンフィグレーションサービスを提供していない可能性がある。

【0088】そのような場合、OAサーバはネットワークに対してコンフィグレーションサービスの提供を開始する。一方、OAサーバがDHCPDISCOVERに対するDHCPOFFERを受信した場合、別の(第2の)デバイスが既にコンフィグレーションサービスをネットワークに提供している可能性がある。そして、OAサーバが、コンフィグレーションサービスをネットワークに提供しているその別のデバイスがOAサーバではないと判定する場合、OAサーバは同様なコンフィグレーションサービスについては提供しないが、その代わりにクライアントOAのように機能する。

【0089】一方、OAサーバが、その別のデバイスがOAサーバであると判定する場合、二つのOAサーバはそれらのうちのいずれがより高い優先順位を有しているかを判定する。高い優先順位を持つOAサーバはマスタサーバとして指定され、低い優先順位を持つOAサーバはクライアントOAとして指定される。ある状況においては、二つのOAサーバが、どのOAサーバがマスタサーバとなるべきかを判定することができない場合があり、ユーザの介入を必要とする。一実施の形態において、そのような状況はほとんど発生しない。

【0090】一実施の形態において、コンフィグレーションサービスをネットワークに提供することが可能なOAサーバは、サーバOAと呼ばれる。サーバOAは、状態変数、タイミングおよび通信の組み合わせを使用して、ユーザが介在することなしに自己識別 (self-identification) のタスクを確実に実行する。サーバOAは、一般に以下の4つの状態の一つが割り当てられる。

1) Initial

2) Master

3) Not\_Master

4) Temporary\_Master

【0091】「Initial」の状態は、デバイスが最初に製造された際にサーバOAに割り当てられる。「Master」の状態は、ネットワークにサービスを提供するあらゆるサーバOAに割り当てられる。「Not\_Master」の状態が割り当てられたサーバOAは、特定の時間においてネットワークにサービスを提供しないという以外、サーバOAであるとしてコンフィグレーションされている。「Temporary\_Master」の状態が割り当てられたサーバOAは、マスタサーバが利用できない場合に一時的にサービスを提供するために指定されるものである。ブートストラップ前の特定のサーバOAの以前の状態を判定し、キャプチャすることが重要である。ブートストラップ後のそのサーバOAの状態も同様である。一実施の形態において、OAの状態変数は、ブートストラップの際に読み取り可能な電子ファイルに定義される場合がある。

【0092】図3は、サーバOAのアーキテクチャの一実施の形態を示す図である。図3において、サーバOA402はネットワーク401に接続されている。なお、ネットワーク401は、インターネット、イントラネット、複数のデバイスが情報を共有可能な他のあらゆる相互接続データバス等、いかなるものであっても良い。オプションとしてネットワーク401に接続されているものとして、クライアントOA400、ユーザサーバ404、マスタサーバ408、サービスディスカバリ (service discovery) を提供するサーバOA、即ちSOAサーバ406および非OAサーバ410が示されている。オプションの接続はネットワーク401に常に接続されていることが要求されないデバイスを示しているが、ある状況においてネットワーク401に接続される場合があるものである。

【0093】図4は、サーバOAの自己識別ルーチンの一実施の形態を示す図である。図4において、そのブートストラップシーケンスを開始すると、サーバOA402はサーバOAとして動作すべきか否か、およびネットワークコンフィグレーションサービスをネットワーク401に提供すべきか否かを判定し、または、クライアントOAとして動作すべきか否か、およびネットワークコンフィグレーションサービスをネットワーク401に提供すべきではないか否かを判定する。そのような判定処理はサーバOA402の状態変数を参照することによって実行される。一実施の形態において、状態変数はシステム自身で設定されるものである。一実施の形態において、ユーザは状態変数をマスタとして選択することによって、状態変数がマスタ状態に設定されるようにする。

【0094】第1の問合せは、サーバOA402がMasterと等しい状態変数を有するか否かである (S50

1)。サーバOA402の状態変数がMasterと等しい場合、サーバOA402は、コンフィグレーションサービスをネットワーク401に提供するステップS525で適切にブートを継続する。ステップS501において、サーバOA402の状態変数がMasterと等しくない場合、状態変数はNot\_Master, Temporary\_MasterおよびInitialのいずれかに等しいということになる。サーバOA402は、時間間隔D毎に(S504)ステップS502においてネットワーク401全体にDHCPDISCOVERを発行(ブロードキャスト)する。この処理は、ステップS506においてDHCP OFFERを受信されるか、またはステップS508においてDHCP応答のために割り当てられた予め設定された時間が満了(経過)するまで続けられる。

【0095】DHCP応答のために割り当てられた時間は、競合しているDHCP構成のサーバ間における競合状態を避けるために、複数のサーバOA全体にわたって変化をつけるようにすることが重要である。DHCP応答のために割り当てられた時間が一定に保たれる場合、(複数の)サーバOAは正しく機能しない場合がある。たとえば、複数のサーバOAがネットワーク上に存在しており、そのような全てのサーバOAが同時にオンされる(たとえば、パワーロスからのリカバリの場合において)ような場合、全てのサーバOAはDHCPDISCOVERを同時に送出する可能性があると考えられる。

【0096】また、全てのサーバOAがDHCPDISCOVERを同時に送出するような場合、全てのサーバOAは返信されるDHCP OFFERの受信を待つことになる。全てのサーバOAがDHCP OFFERの受信を待っているような場合、サーバOAのいずれも期待されるDHCP OFFERを送信することはできない。そのような状況において、DHCP応答のために割り当てられた予め設定された時間は、全てのサーバOAにおいて同時に経過(満了)することになる。

【0097】さらに、各サーバOAは、それぞれそれぞれ自身がネットワーク上に単独で存在していると判断し、ネットワークに対してコンフィグレーションサービスの提供を開始することになる。しかし、DHCP応答のために割り当てられている時間が変えられる(多様にできる)ような場合、少なくとも一つのサーバOAがネットワークに対してコンフィグレーションサービスの提供を開始することになる。DHCPDISCOVERが繰り返される間隔より大きな時間までその時間に変化をつけることが重要である。一実施の形態において、変化はそのサイズが繰り返し速度に等しい特定の量である。それは秒数の場合がある。

【0098】再び図4に戻り、サーバOA402の状態変数がMasterと等しくないとステップS501で判定されると共に、サーバOA402がステップS502でDHCPDISCOVERをネットワーク401全体にブ

ロードキャストした後のつぎの間合せは、サーバOA402がステップS506でDHCP OFFERを受信したか否かを判定することである。サーバOA402が、DHCP応答のために割り当てられた予め設定された時間がステップS508において経過する前にステップS506でDHCP OFFERを受信した場合、サーバOA402の状態変数はステップS510でNot\_Masterに設定され、そしてサーバOA402はステップS511においてクライアントOAのように動作し続ける。

【0099】サーバOA402がそのDHCPDISCOVERに対する応答を受信した場合、コンフィグレーションサービスをネットワーク401に提供する別のデバイスがネットワーク401に存在していると推定される。そのような場合、サーバOA402は、行うことは可能ではあるが、コンフィグレーションサービスをネットワーク401に提供しない。

【0100】サーバOA402がDHCP応答のために割り当てられた予め設定された時間がステップS508で経過する前にDHCP OFFERをステップS506で受信しなかった場合、コンフィグレーションステップS530が実行される。コンフィグレーションステップS530において実行される第1の判定処理は、サーバOA402の状態変数がInitialと等しいか否かである(S512)。サーバOA402の状態変数がステップS512においてInitialと等しく、DHCP応答のために割り当てられた予め設定された時間が経過した場合、サーバOA402の状態変数はステップS520においてMasterにセットされる。

【0101】サーバOA402は、コンフィグレーションサービスをネットワーク401に提供するステップS525において適切にブートを継続する。そのような状況において、サーバOA402は、ネットワーク401に接続される際にそのデフォルトの出荷状態にあり、そして、コンフィグレーションサービスをネットワーク401に提供しているため、他のいかなるデバイスも検出されなかった可能性がある。

【0102】図4におけるコンフィグレーションステップS530において、サーバOA402の状態変数がMasterまたはInitialと等しくなく、かつ、DHCP応答のために割り当てられた予め設定された時間が経過した場合、ステップS514においてユーザの介入が要求される場合がある。ユーザの介入が要求された場合、ユーザはサーバOA402の適切な状態変数がMaster, Temporary\_MasterおよびNot\_Masterのいずれかを選択するように促される。サーバOA402がネットワーク401に接続される前に、他の若干のデバイスがコンフィグレーションサービスをネットワーク401に提供している可能性が常にある。

【0103】そのようなデバイスは偶然にオフにされたものである場合があり、またはある時点で機能的な問題

に直面したものである場合がある。たとえば、他のデバイスが故障し、もはやコンフィグレーションサービスをネットワーク401に提供することができない場合、ユーザはサーバOA402の状態変数をMasterおよびTemporary\_Masterのいずれかにセットするように促される。他のデバイスが誤ってオンされなかった場合、ユーザはサーバOA402の状態変数をMaster、Temporary\_MasterおよびNot\_Masterのいずれかにセットするように促される。

【0104】ユーザがステップS518でNot\_Masterを選択する場合、サーバOA402はステップS502において再びDHCPDISCOVERのブロードキャストを開始する。ユーザがTemporary\_Masterを選択する場合、サーバOA402はマスタサーバが見つけれらるまでの間だけコンフィグレーションサービスを提供する。ユーザがMaster状態を選択する場合、サーバOA402は、コンフィグレーションサービスをネットワーク401に提供するステップS525においてブートを継続する。

【0105】図5は、サーバOAの自己識別ルーチンの代替的な実施の形態を示す図である。図5において、コンフィグレーションステップS530は、コンフィグレーションステップS531に置き換えられている。図5において、DHCP OFFERがステップS506で受信されず、かつ、DHCP応答のために割り当てられた時間がステップS508で経過したと判定されると、コンフィグレーションステップS531が実行される。

【0106】サーバOA402の以前の状態変数がステップS513でNot\_Masterと等しい場合、状態変数はステップS517でTemp\_Masterにセットされる。サーバOA402の以前の状態変数がステップS513でNot\_Masterと等しくない場合、以前の状態変数がステップS515においてInitialと等しいか否かが判定される。サーバOA402の以前の状態変数がステップS515においてInitialと等しい場合、状態変数はステップS519でMasterにセットされる。サーバOA402の以前の状態変数がステップS515でInitialと等しくない場合、サーバOA402は、コンフィグレーションサービスをネットワーク401に提供するステップS525において適切にブートを継続する。

【0107】サーバOA402の状態変数が、ステップS517およびS519のそれぞれにおいてTemporary\_MasterおよびMasterのいずれかに適切にセットされると、サーバOA402はステップS525において適切にブートを継続する。以降のブート処理は図6に示されている。図6において、サーバOA402は、ステップS602においてIPアドレスのプールからIPアドレスを選択する。一実施の形態において、サーバOA402は、最初に以前使用されていたIPアドレスを、それが存在している場合に選択しようとする。

【0108】IPアドレスが選択された後、サーバOA402は、ステップS604において、選択したIPアドレスが使用可能であるか否かを判定する。一実施の形態においては、ARP (Address Resolution Protocol) がそのような判定を行うために使用される。そのIPアドレスが使用可能でない場合、サーバOA402は、ステップS602においてアドレスのプールから別のIPアドレスを選択する。

【0109】一方、選択したIPアドレスが利用可能であると判定される場合、サーバOA402は、ステップS608においてDHCPサービスを開始すると共に、ステップS610においてDNSおよびサービスディスカバリ (service discovery; SD) を開始する。適切なサービスが開始された後、サーバOA402は、ステップS612においてDHCPDISCOVERをネットワーク401全体にブロードキャストし、そしてステップS614においてDHCPDISCOVERに対応してDHCP OFFERが受信されたか否かを判定する。

【0110】サーバOA402がステップS614においてDHCP OFFERを検出するような場合、別のデバイスがコンフィグレーションサービスをネットワーク401に提供することを開始していたようであり、そしてサーバOA402はステップS616においてグレースフルシャットダウン (graceful shutdown) 手順を実行する。反対に、サーバOA402がステップS614においてDHCP OFFERを検出しないような場合、他のいかなるサーバデバイスもコンフィグレーションサービスをネットワーク401に提供していないようである。そのような場合、サーバOA402は、DHCP OFFERがステップS614で受信されるまでステップS612においてDHCPDISCOVERを送信し続ける。

【0111】DHCPコンフィグレーションは、TCP/IPオプションフィールドを含む場合がある。OAの環境において、あるオプションフィールドがサーバOAを分類するために使用される。あるサーバOAは、High\_Priority\_ServerおよびOrdinary\_Serverのいずれかに分類され得る。複数のサーバOAがネットワークに接続されている場合、コンフィグレーションサービスをネットワークに提供するサーバOAがHigh\_Priority\_Serverとして指定される。

【0112】Ordinary\_Serverとして指定されるサーバOAはほとんどクライアントOAのように機能する。典型的に、任意の与えられた時間に特定のネットワークに接続されるHigh\_Priority\_Serverはたった一つしかない。High\_Priority\_Serverは、ユーザによって選択されたサーバであっても良い。DHCP OFFERのフィールド中の識別子は、そのサーバがHigh\_Priority\_Serverであるか否かを示すためにセットされる。一実施の



形態において、High\_Priority\_Serverは全ての他のサーバにそのアドレスまたは識別子を通知する。

【0113】図7は、グレースフルシャットダウン手順の一実施の形態を示す図である。図7において、DHCPは新たなリース期間(lease)は認められないと通知される(S630)。そして、リース期間が満了していないまま存在しているか否かが判定される(S632)。DHCPリースはタイムリミットを有し、OAは比較的短いもの(たとえば1分)を保持している。ステップS632で存在していると判定された場合、処理ループはリース期間が未だ満了していないか否かを調査する処理に戻る。全てのリース期間が満了している場合、DNSおよびDHCPはシャットダウンされ(S634)、そして、サーバOAはDNS/DHCPクライアントとしての動作を開始する(S636)。

【0114】【ネットワークアドレスおよびネットワーク名の管理】OAデバイスは、たとえそのアドレスが変わったとしてもホスト名が変わることは滅多にないように、DHCPおよびDNSサービスと一緒に機能するような方法を使用する。OAのアーキテクチャはネットワーク名を一貫したものにしておこうとし、さらにネットワーク名の競合を解決する方法を使用する。従来より、ユーザまたはネットワーク管理者は、ネーミングの競合を避けるためにホストのネットワーク名をマニュアルで割り当て、または変更することが任されている。これとは対照的に、OAのアーキテクチャは、これらのサービスを自動化し、それによってエラーのリスクはもちろん、ユーザの介入の必要性を減少させる。

【0115】一実施の形態において、DHCPサーバは、サーバOA402上に実装されると共に、ネットワーク名の競合および割り当てを記録するテーブルを含んでいる。なお、このテーブルはバインディングと呼ばれるものである。DHCPテーブルは、あるデバイスのMAC(Media Access Control)アドレスを、そのデバイスの対応するネットワーク名バインディングと共に記録する。MACアドレスはネットワークの各ノードをユニークに識別するハードウェアアドレスである。デバイスのMACアドレス以外の別の識別子は、異なるネットワークテクノロジーが実装される場合に識別目的のために使用されると考えられる。

【0116】また、デバイスのMACアドレス、およびネットワークまたはホスト名バインディングと共に、テーブルは、「name\_in\_use」コードはもちろん、デバイスのIPアドレスのような情報のためのフィールドを含む。name\_in\_useコードはブートストラップの際に初期化されるものであり、特定のホスト名が別のデバイスで使用されているか否かを示すものである。

【0117】図8は、OAの名前およびアドレス管理の一実施の形態を示すフローチャートである。図8において、そのブートストラップシーケンスを開始すると、ク

ライアントOA400はコンフィグレーション情報をサーバOA402から取り出そうとする。ステップS702において、クライアントOA400は、クライアントOA400をコンフィグレーションする際に使用するため、サーバOA402のために所望のIPアドレスおよびホスト名を提示する。ステップS704において、サーバOA402はクライアントOA400のMACアドレスを取得し、続いてステップS706においてそのMACアドレスがサーバOA402のDHCPテーブル中に存在しているか否かを判定する。

【0118】クライアントOA400のMACアドレスがDHCPテーブルに存在しているような場合、サーバOA402は、クライアントOA400の以前の名前およびアドレスバインディングをステップS708で読み出す。一方、クライアントOA400のMACアドレスがDHCPテーブルに存在していないような場合、サーバOA402はステップS710でクライアントOA400のエントリを生成する。ステップS712において、サーバOA402はDHCPテーブルのnot\_in\_useフィールドを調査し、クライアントOA400の選択されたネットワーク名が別のデバイスによって既に使用されているか否かを判定する。

【0119】そのネットワーク名が別のデバイスによって既に使用されているような場合、サーバOA402は、ステップS714において選択されたネットワーク名を修正する。ネットワーク名を修正した後、サーバOA402は、新たに修正されたネットワーク名も使用中であるか否かを判定する。サーバOA402は、適当な名前が発見されるまでクライアントOA400のネットワーク名の修正およびチェックを継続する。ステップS712において、サーバOA402はクライアントOA400のネットワーク名が既に使用中ではないと判定した場合、その後サーバOA402は、ステップS720においてクライアントOA400のIPアドレスが別のデバイスによって使用されているか否かを判定する。

【0120】クライアントOA400のIPアドレスが別のデバイスによって使用されている場合、サーバOA402はステップS722においてクライアントOA400のIPアドレスを修正する。クライアントOA400のIPアドレスが修正された後、サーバOA402は新たなIPアドレスも別のデバイスによって使用されているか否かを判定する。サーバOA402は、適当なIPアドレスが確かめられるまで、この方法でクライアントOA400のネットワークIPアドレスを割り当てると共にチェックし続ける。

【0121】適当なネットワーク名およびネットワークIPアドレスが決定された後、DHCPテーブル中の全てのフィールドは、ステップS724において該当する情報を用いて完成される。ステップS726において、サーバOA402は、クライアントOA400に割り当

てられたネットワーク名が使用中であることを示すname\_in\_useフィールドに任意のマークを記録する。このように、そのネットワーク名がクライアントOA400に割り当てられている間、他のあらゆるデバイスはこのネットワーク名を使用しようとはしないであろう。

【0122】ステップS728において、この特定の実施の形態においてサーバOA402であるDHCPサーバは、この特定の実施の形態においてはまたサーバOA402であるDNSサーバにネットワーク名およびIPアドレスの割り当てを通知する。そして、サーバOA402は、ステップS730においてコンフィグレーション情報をクライアントOA400にDHCP OFFERを介して返信する。そのようなコンフィグレーション情報は、クライアントのネットワーク名、IPアドレス、ドメイン名、DNSサーバアドレスおよびルータアドレスを含んだものであっても良い。ステップS732において、サーバOA402はDHCPDECLINEがクライアントOA400から返信されて来たか否かを判定する。

【0123】DHCPDECLINEが返信されて来た場合、サーバOA402は、ステップS733においてなぜコンフィグレーションが拒絶されたのかを判定するようにユーザに警告することができる。サーバOA402がDHCPDECLINEを受信しない限り、クライアントOA400がコンフィグレーション情報を受け入れたと推定され、ステップS736においてサービスディスカバリ(servicediscovery)を開始する。

【0124】この名前およびアドレス管理コンフィグレーション手順において説明したクライアントはクライアントOAであると仮定したが、DHCPコンフィグレーションを受け入れることができるように構成された非OAクライアントにそのようなコンフィグレーション手順を適用することも可能である。サーバOA402がコンフィグレーション情報を非OAクライアントに返信するようになっている場合、サービスディスカバリは実行されない場合があり、名前およびアドレスコンフィグレーション手順はステップS738で終了する。

【0125】〔名前の修正〕DHCPクライアントがホスト名をDHCPサーバに送信する場合、そのホスト名が既に使用中である可能性がある。このとき、DHCPサーバはホスト名をユニークなものとなるように変更する。

【0126】一実施の形態において、以下のプロセスがホスト名の競合を解決する。

1. リクエストされたホスト名が所定の文字数(たとえば15)より短い場合、桁数(number digits)をその末尾に加える。
2. ユニークなホスト名を作るために上記ステップ1では不十分な場合、修正されたホスト名の最後の文字をアルファベット順でインクリメントする。

3. 最後の文字がaからzまでチェックされ、そして修正したもの全てがユニークではない場合、最後から2番目の文字が数字/アルファベット順でインクリメントされ、そして最後の文字は0~9やa~zにわたって修正される。

4. 一実施の形態において、このプロセスは、決してマイナスを加えたり、文字を強調するようなものではない。

5. オリジナルの文字がマイナスまたは強調された文字である場合、つぎの文字は0である。

【0127】〔アドレスの範囲〕OAの一実施の形態において、クラスAのプライベートアドレスの範囲として、以下のようなものが使用される。

10. xxx. yyy. 0~10. xxx. yyy. 255

【0128】「xxx. yyy」で示されたセクションがOAで使用され、新たなDHCPサーバがオリジナルのOAサーバから引き継ぐ場合にサーバがクライアントをスムーズに転送することを可能にする。

【0129】DHCPサーバは、以下のアドレスの範囲からクライアントアドレスを割り当てる。

10. xxx. yyy. 100~10. xxx. yyy. 200

【0130】このアドレスの範囲はDHCPサーバ自体のアドレスを含み、DHCPサーバは最大100のアドレスを割り当てることができることを意味している。若干の静的なアドレスの割り当てを望んでいるが、大部分は各OAがそれらをコンフィグレーションすることを可能にすることを望んでいるネットワーク管理者は、以下の範囲を静的な割り当てのために使用することができる。

10. xxx. yyy. 0~10. xxx. yyy. 99

10. xxx. yyy. 201~10. xxx. yyy. 255

【0131】一実施の形態において、自動的にコンフィグレーションされるOAネットワークのネットワークマスクは、255. 0. 0. 0である。

【0132】〔サービスディスカバリ〕OAネットワークアーキテクチャは、自動サービスディスカバリ(発見)機能(automatic service discovery feature)を提供する。SOAサーバは、サービスディスカバリ機能をネットワークに提供することに対して責任を有している。SOAサーバは、ネットワーク上の各OAデバイスのサービス名を記述しているサービスリストを収集する。このサービスリストを使用することにより、各OAは、それ自体をネットワーク上の他のOAと簡単に関連付けすることができる。

【0133】典型的なSOAサーバは、HTTP(hypertext transfer protocol)デーモンおよびHTTPクエリーを発行するプログラムの組み合わせである。一実施の形態において自動コンフィグレーションが望まれている場合、SOAサーバはマスタサーバ上に置かれる。別の実施の形態において自動コンフィグレーションが望

まれていない場合、またはSOAサーバが管理されている環境に位置している場合、SOAサーバをマスターサーバ以外の別々のデバイス上に置くこともできる。

【0134】一実施の形態において、SOAサービスリストは人間が判読可能なテキストデータを使用して構成される。各テキスト行はフォーム「service: <:servicename>:: //<:FQDN>:」に似ている。ここで、<:servicename>:は、OAが提供するサービスの種類を示し、<:FQDN>:は、十分に必要条件を備えたドメイン名（fully qualified domain name）を示している。ホスト名の命名規則は必要とされないのに対し、サービス名用の命名規則を保持することは賢明である。

【0135】一実施の形態において、SOAサーバは、HTTPクエリーを使用して各OAの個々のサービスリストをリクエストすることによってマスターサービスリストを編成する。HTTP（hypertext transfer protocol）構文およびSLP（service location protocol）構文の両方を使用してこの結果を得ることができる。SLP（サービスの定義）

名称	意味
doc_capture	accepts documents for archiving
doc_retrieval	allows retrieval of archived documents
lpr	accepts print jobs
fax_send	accepts fax pages to send
calendar_schedule	schedules a calendar entry
calendar_retrieval	retrieves a calendar entry

【0139】上記の例において、サービス名「doc\_capture」を有するOAデバイスは、ネットワークを通じてアーカイブの目的のために文書を受け入れる場合がある。代表的な十分に必要条件を備えたドメイン名（FQDN）は、「archive.<:domainname>:」であり、「archive」はOAデバイスがアーカイブの種類のようなものであることを示し、「<:domain name>:」はOAデバイスが接続されるネットワークのローカルドメイン名を指すものである。同様に、プリントジョブを受け入れるプリンタと指定されるOAデバイスは、「lpr」というサービスを提供することができる。対応するサービスリストのエントリは、「lpr://printer.<:domain name>:」のようなものである。

【0140】SOAがHTTPクエリーを使用して各OAの個々のサービスリストをリクエストすると、各OAは応答しなければならない。SOAのクエリーに応じてOAによって返信される代表的なサービスリストは、以下のようなものである。

【0141】

```
service: doc_capture://
service: doc_retrieval://
service: lpr://
```

【0142】各OAによって返信されるサービスリストのフォーマットはSOAのサービスリストに類似したも

P（service location protocol）構文の詳細な情報については、RFC 2165, "Service Location Protocol", June 1997で得ることができる。

【0136】HTTPベースのサービスリストの例は、サービスの定義と共に、以下から得られる。

【0137】（サービスリスト）

```
service: doc_capture://archive.<:domain name>;
service: doc_retrieval://archive.<:domain name>;
service: lpr://archive.<:domain name>;
service: lpr://printer.<:domain name>;
service: doc_retrieval://printer.<:domain name>;
service: fax_send://fax.<:domain name>;
service: calendar_schedule://calendar.<:domain name>;
service: calendar_retrieval://calendar.<:domain name>;
```

【0138】

のであるが、冗長なFQDN情報は渡されない。

【0143】一実施の形態において、クライアントOAがサービスディスカバリを開始する場合、クライアントOAは、そのブートストラップシーケンス内においてHTTP POSTコマンドを使用してそれ自身のサービスリストをSOAサーバにプッシュする。いずれのデバイスがDNSおよびDHCPサービスをネットワークに提供するかににより、二つのハンドシェーキング手順（handshaking procedure）のうちの 하나가始まる。

【0144】一実施の形態において、OAデバイスがDNSおよびDHCPサービスをネットワークに提供する場合、そのネットワーク上の全てのOAデバイスはSOAサーバの別名がデフォルトでSOA.DOMAINであることを認識している。特定のDOMAINが要求されないような場合、「local」がその場所に使用される。そのような場合、各OAはそれらのサービスリストをHTTP POSTを使用して以下に示すURL（uniform resource locator）にプッシュする。

http://SOA.local/SOA\_service\_list

【0145】このような状況において、「SOA」は特定のOAの名称であり、「local」は現在のネットワークドメインを指し、「SOA\_service\_list」はOAによってプッシュされたサービスリストを受け入れる機構にリンクされるものである。CGI（common gateway inter

face) プログラムは所望の結果を達成する一つの機構である。

【0146】代替的な実施の形態において、既存の非OAデバイスまたは複数のデバイスがDNSおよびDHCPサービスをネットワークに提供するという場合、ネットワークは管理されている可能性が非常に高い。このような例において、ネットワーク管理者は、SOAサーバの別名と共に、SOAサーバのDNSエントリをマニュアルでDNSに加える。DHCPサーバによって与えられた「SOA」および「DOMAIN」名を結びつけることによって他のOAデバイスがSOAサーバを参照できるように、SOAサーバの名前は「SOA」であることが好ましい。名前「SOA」が既に使用されている場合のようなまれな状況において、全てのOAデバイスが正しいURLをポイントできるように構成されている限り、任意の名前を選択することができる。

【0147】OAがそのサービスリストをSOAサーバにプッシュすると、SOAサーバはサービスリストを登録すると共に、OAクライアントの名前を記憶する。OAサービスに対するつぎの変更が行われる場合、SOAサーバ中に保持されているサービスリストがアップデートされる。より詳細に、新たなOAデバイスがネットワークに加えられた場合、そのOAデバイスはそのサービスリストをSOAサーバにプッシュし、そしてSOAサーバはこの情報を記憶している他のクライアントOAの全てに配信する。これは、たとえば以下のようなURLにクライアントをプッシュすることによって実現し得る。

`http://HOST.DOMAIN/OA_service_list`

【0148】ネットワーク管理者が複数のOAをいくつかのプロジェクトまたは組織的なワークグループに分けることを望む場合、そのネットワーク管理者は、所望の特定のSOAサービスに関するそれぞれのURLを定義することによってワークグループを維持することができる。たとえば、ネットワーク管理者が、サービスリストを管理するためにOAのあるグループに単一のサーバを用意することを決定する場合、ネットワーク管理者は、ワークグループ内において単一のURLをポイントするように各OAをコンフィグレーションすることができる。

`http://SOME_SERVER.DOMAIN/OA_Service_List_For_Workgroup_3`

【0149】同様に、単一のサーバ上の異なるURLをポイントするように、異なるワークグループをコンフィグレーションすることができる。

`http://SERVER1.DOMAIN/OA_Service_List_For_Workgroup_4`

`http://SERVER1.DOMAIN/OA_Service_List_For_Workgroup_5`

`http://SERVER1.DOMAIN/OA_Service_List_For_Work`

`group_6`

【0150】【ユーザの識別】OAの機能を利用するために、ユーザ名を最初に入力し、続いてパスワードを入力することが必要である。ここでユーザ名には、個人名とグループ名という典型的な二つの種類のユーザ名がある。グループ名はそのグループにアクセスすることが許可されたメンバーのリストを含み、一方、個人名はメンバーを持たないグループ名の特別なケースとみなされる場合がある。ユーザおよびパスワード情報が保存されるファイルフォーマットは重要ではない。OAシステムは、利用されるファイルフォーマットにかかわらず、アプリケーションプログラムにインタフェースを提供する。

【0151】一実施の形態において、ユーザデータベースの最初のラインは、特定のファイルフォーマットまたはこのファイルで使用される文字符号化(character encoding)を指定するコードである。ユーザデータベースのつぎの行は、ユーザデータベースが最後に変更された時間および日付を表すタイムスタンプである。タイムスタンプは、以下のようなフォーマット中に見かけ得る。

{YYYYMMDDHHMMSS}

【0152】ここで、YYYYは年を示し、MMは月を示し、DDは日を示し、HHは時間を示し、MMは分数を示し、SSは秒数を示し、これらはユーザデータベースが最後に変更された際のものである。一実施の形態において、日付および時間はグリニッジ標準時(GMT)で記録される。

【0153】タイムスタンプの後において、OAユーザデータベースはユーザおよびグループを表すエントリのリストを含んでいる。ユーザエントリは、ID、フルネーム、クリアテキストパスワードおよびそのユーザがメンバーとなっているグループのリストを含むものである。一方、グループエントリは、ユーザがメンバーとなっているグループのリストを含むものであるが、ユーザエントリに含まれているパスワードや他の情報については含まれていない。ユーザデータベースの6つのラインの例を以下に示す。

【0154】

```
admin0A:Administrator:adminpassword:
user1:User Name 1:user1password:admin,group1,group
2
user2:User Name 2:user2password:group1
group1:Group Name 1:
group2:Group Name 2:
group3:Group Name 3:group2
```

【0155】パスワードは、同様な環境における普通のやり方と同様に暗号化されたフォーム中ではなく、OA上のクリアテキストフォーム中に保存される。このようにされるのは、個々のパスワードが、いくつかのOAのための多重パスワードハッシュ方式(multiple passw

ord hashing schemes) の下において再利用されることを必要とするからである。しかし、OAどうしの間でユーザデータベースを転送する場合には暗号化される。そのような暗号化機構は、OAのように見せかけているホストが、何らかの種類のセキュリティコードを得ることなしに、アクセスを許可されないことを確実にする。問題のデバイスが同様のプロトコルを使用して暗号キーを生成する限り、使用される特定の暗号化アルゴリズムは重要ではない。

【0156】図9は、パスワード配信ルーチンの一実施の形態を示すフローチャートである。パスワード配信を含むユーザ識別手順は、いくつかのデバイス上で実行され得る。指定された管理者を欠くネットワーク環境において、ユーザ識別サービスは、SOAサービスと同様のデバイス上に置かれる。SOAサービスはそのようなネットワーク環境においては典型的にマスターサーバ上に置かれるため、ユーザ識別サービスについてもマスターサーバ上に置かれることになる。管理されたネットワーク環境において、ユーザ識別サービスは別々のデバイス、典型的にはユーザサーバと呼ばれるものに置かれる場合がある。

【0157】図9において、OAのネットワークに接続されているクライアントは、ステップS800において、「oa\_request\_users」と呼ばれるCGIプログラムを利用して、マスターサーバからパスワードリストをリクエストする。ステップS801において、マスターサーバは、クライアントOAのセキュリティコードで暗号化された乱数でクライアントOAに要求する(チャレンジ(challenge)する)。これは、oa\_request\_keyと呼ばれるCGIプログラムを使用することで実現される。

【0158】そして、クライアントOAは、ステップS802、S803およびS804において、そのセキュリティコードを使用して乱数を解読し、1をその乱数に加え、そして結果として得られた乱数を再び暗号化する。ステップS805において、クライアントOAは、再度暗号化した乱数をマスターサーバに返送する。ステップS806において、サーバは、クライアントOAによって返送されて来た乱数が返送を期待していた乱数であるか否かを判定する。返送されて来た乱数が期待していた乱数でなく、従って正しいものではない場合、トランザクションはステップS815においてセキュリティを目的としてアボートされる。

【0159】一方、クライアントOAによってマスターサーバに返信された乱数が正しいものである場合、マスターサーバは、ステップS807においてインクリメントされた数字を用いてユーザデータベースを暗号化する。続いて、マスターサーバは、ステップS808において、HTTPを介して暗号化されたユーザデータベースをポストし、accept\_userdbと呼ばれるCGIプログラムを呼び出す。クライアントOAは、ステップS809におい

て、インクリメントされた乱数を用いてユーザデータベースを解読し、データベース転送ルーチンを完了する。

【0160】これで、クライアントOAは、ユーザデータベース中のタイムスタンプをチェックし、クライアントOAおよびマスターサーバのいずれが最も新しいユーザデータベースを有しているかを判定する。ステップS811において、クライアントOAが最も新しいユーザデータベースのコピーを有していると判定された場合、クライアントOAは、ステップS801～S809を説明したようにして繰り返すことにより、ステップS812においてユーザデータベースの最新のコピーをマスターサーバに送信する。

【0161】そして、マスターサーバは、ステップS801～S812を説明したようにして繰り返すことにより、ステップS813においてネットワーク上の全ての他のクライアントOAに最も新しいデータベースをプッシュする。ステップS811において、マスターサーバがユーザデータベースの最も新しいコピーを有していると判定された場合、クライアントOAがそのユーザデータベースをマスターサーバに送信する必要はない。そして、マスターサーバは、ステップS801～S812を繰り返すことにより、そのユーザデータベースをネットワーク上の全ての他のクライアントOAにプッシュする。

【0162】なお、他のパスワード配信ルーチンを使用することも可能である。

【0163】前述した説明を読んだ後に、この技術の当業者にとって、本発明について多くの設計変更を行うことが可能であることは間違いなく明らかになるが、例として開示されたいかなる特定の実施の形態に本発明を限定することを意図したものではないということはあらゆる点からも理解されるであろう。したがって、様々な実施の形態の詳細を参照することは、本発明にとって必須であると考えられる特徴のみが列挙された特許請求の範囲の各請求項の範囲を限定することを意図するものではない。

#### 【0164】

【発明の効果】以上説明したように、本発明によれば、簡単、快適、および家電品のような自動コンフィグレーション機能をユーザに提供するネットワークデバイスを提供することができるというような効果を得ることができる。

#### 【図面の簡単な説明】

【図1】クライアントOAのアーキテクチャの一実施の形態を示す説明図である。

【図2】クライアントOAのコンフィグレーションの一実施の形態を示すフローチャートである。

【図3】サーバOAのアーキテクチャの一実施の形態を示す説明図である。

【図4】クライアントOAのコンフィグレーションの一実施の形態を示すフローチャートである。

【図5】クライアントOAのコンフィグレーションの代替的な実施の形態を示すフローチャートである。

【図6】OAの成功したブート手順の一実施の形態を示すフローチャートである。

【図7】OAのグレースフルシャットダウン手順の一実施の形態を示すフローチャートである。

【図8】OAの名前およびアドレス管理の一実施の形態を示すフローチャートである。

【図9】OAのパスワード配信ルーチンの一実施の形態を示すフローチャートである。

【図10】従来技術に基づく動的なホストコンフィグレーションプロトコルおよびドメインネームサービスサーバを含む従来のネットワークを示す説明図である。

【符号の説明】

100 クライアント

101, 201, 401 ネットワーク

102 ドメイン名

103 IPアドレス

105 DISCOVER

106 OFFER

107 REQUEST

108 ACKNOWLEDGE

110, 111 DHCPサーバ

115, 202 ホスト

118 データベース

120 DNSサーバ

200 クライアントOA

210 非OAサーバ

400 クライアントOA

402 サーバOA

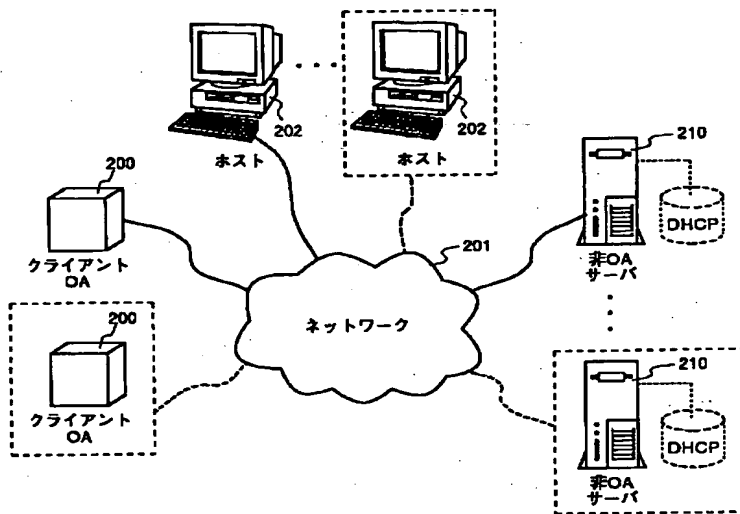
404 ユーザサーバ

406 SOAサーバ

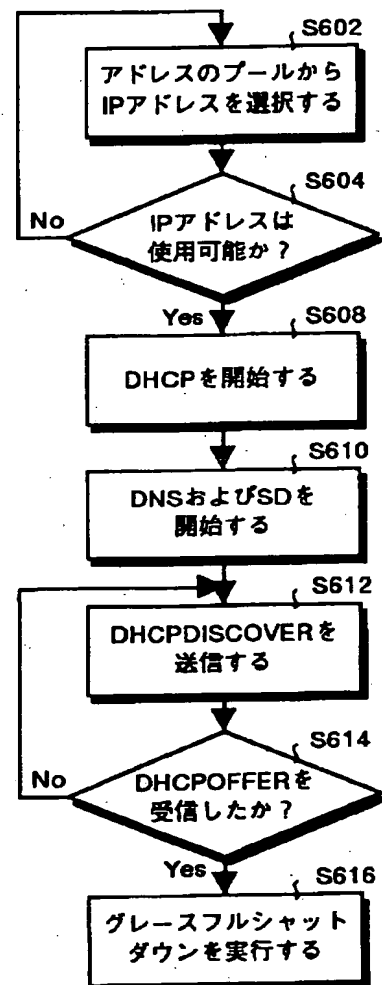
408 マスタサーバ408

410 非OAサーバ

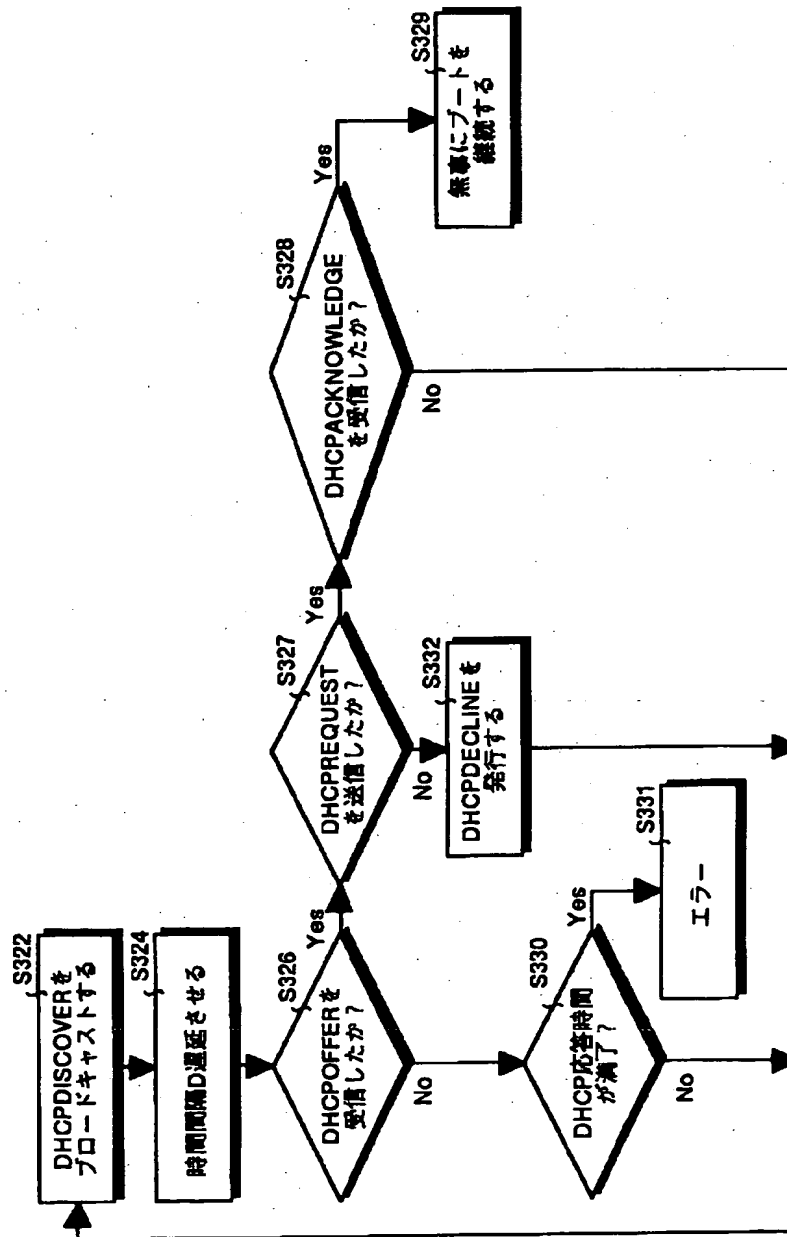
【図1】



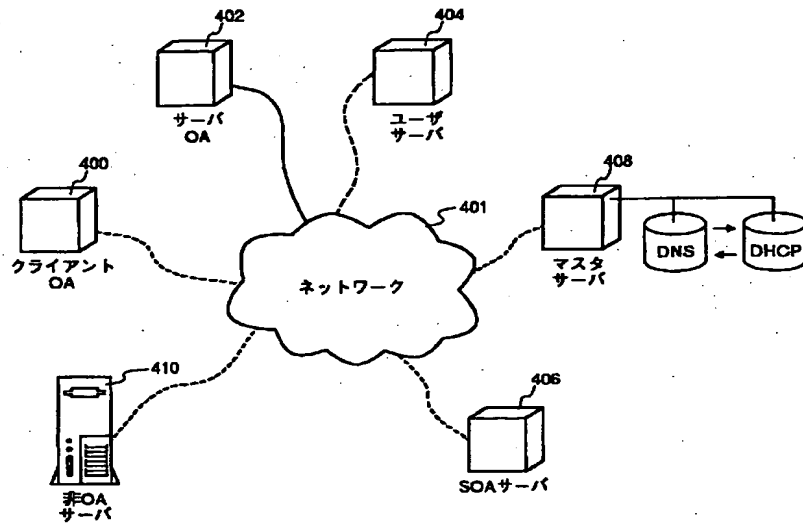
【図6】



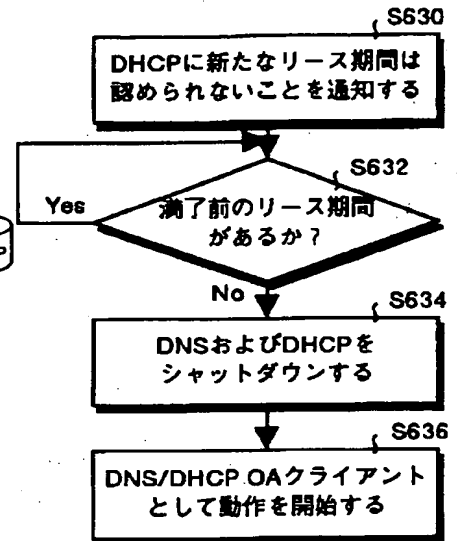
【図2】



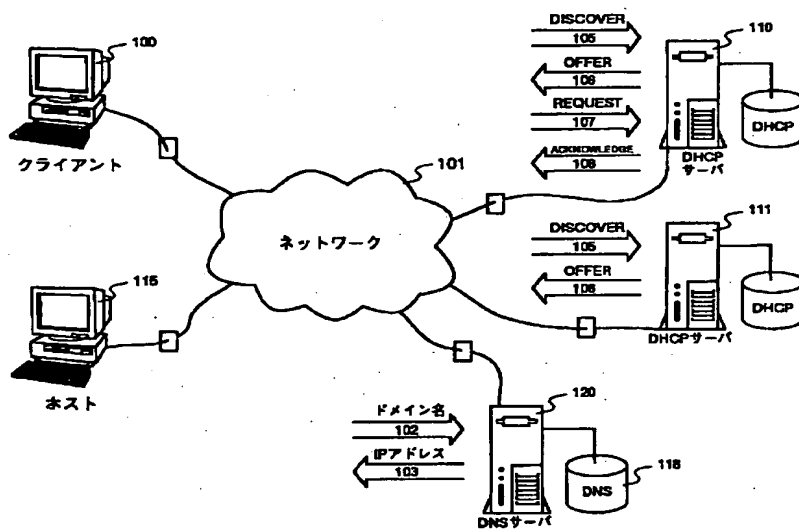
【図3】



【図7】

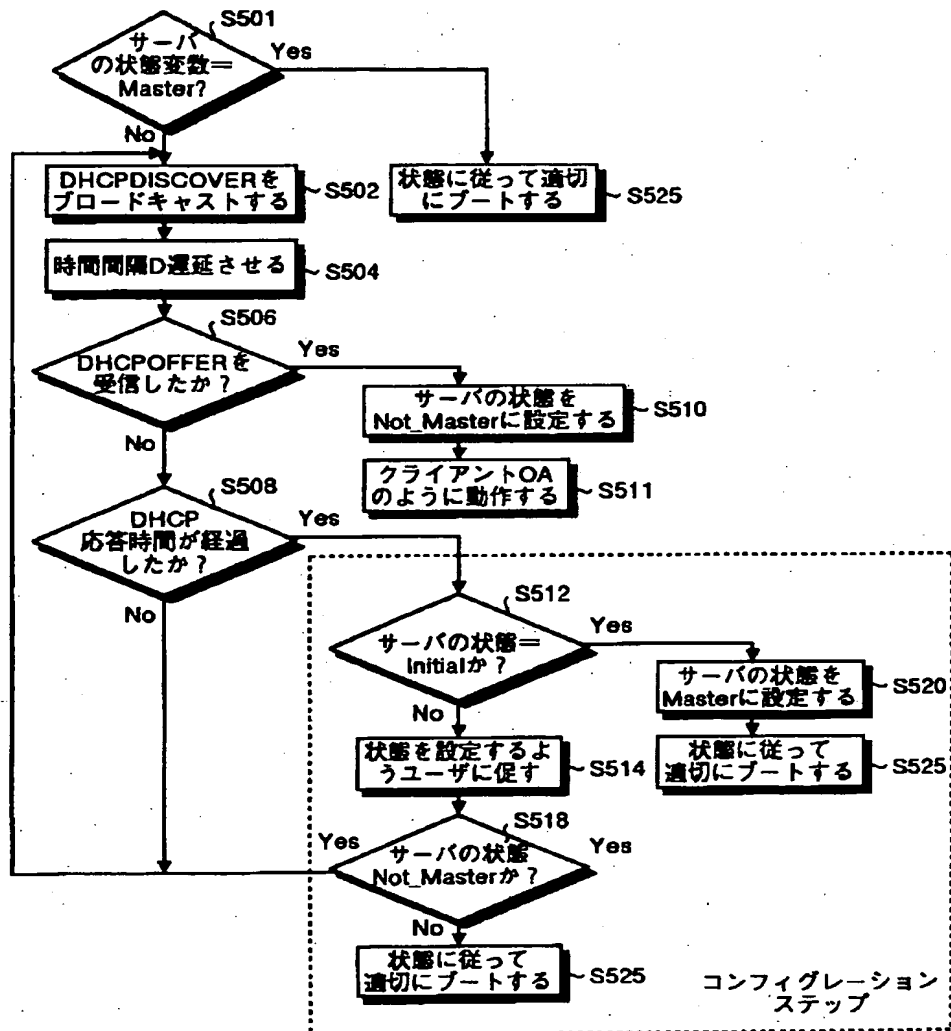


【図10】

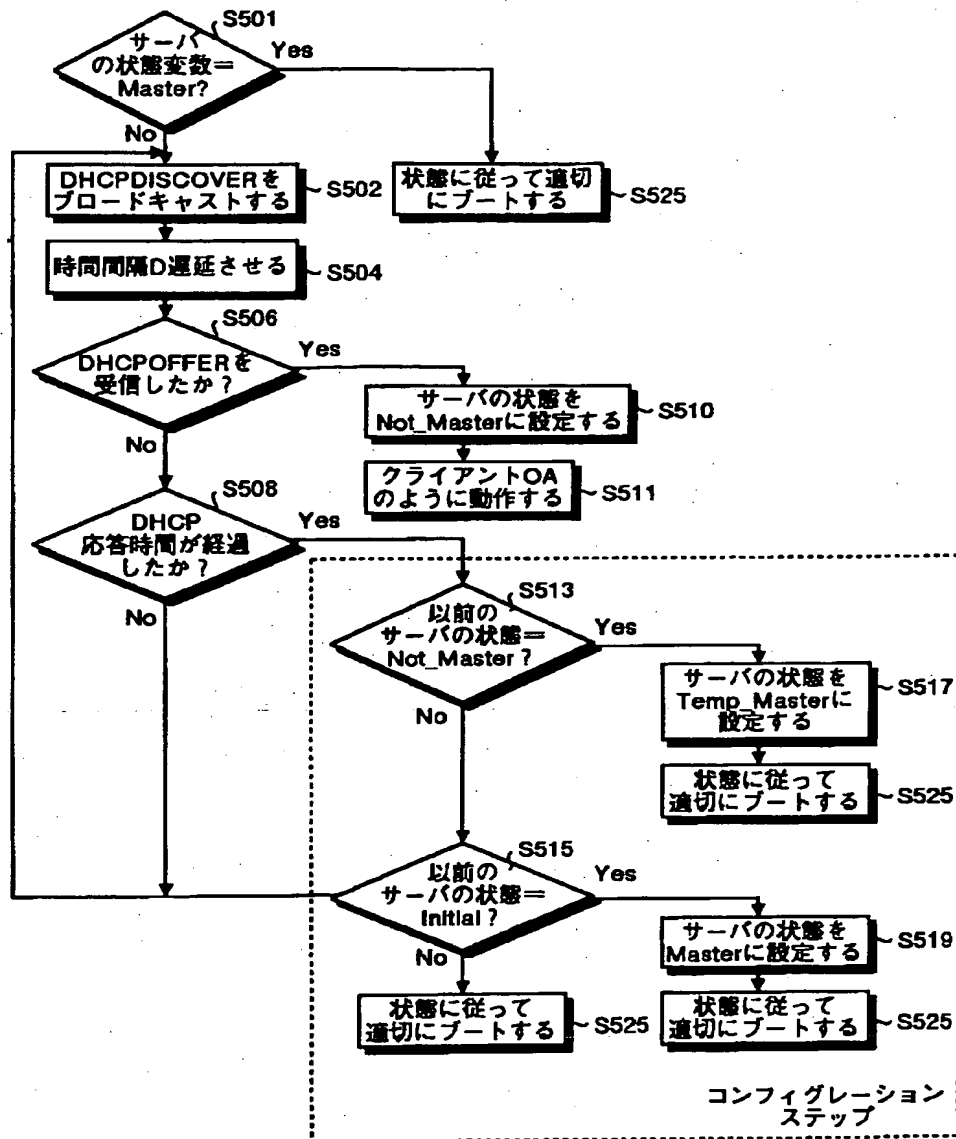




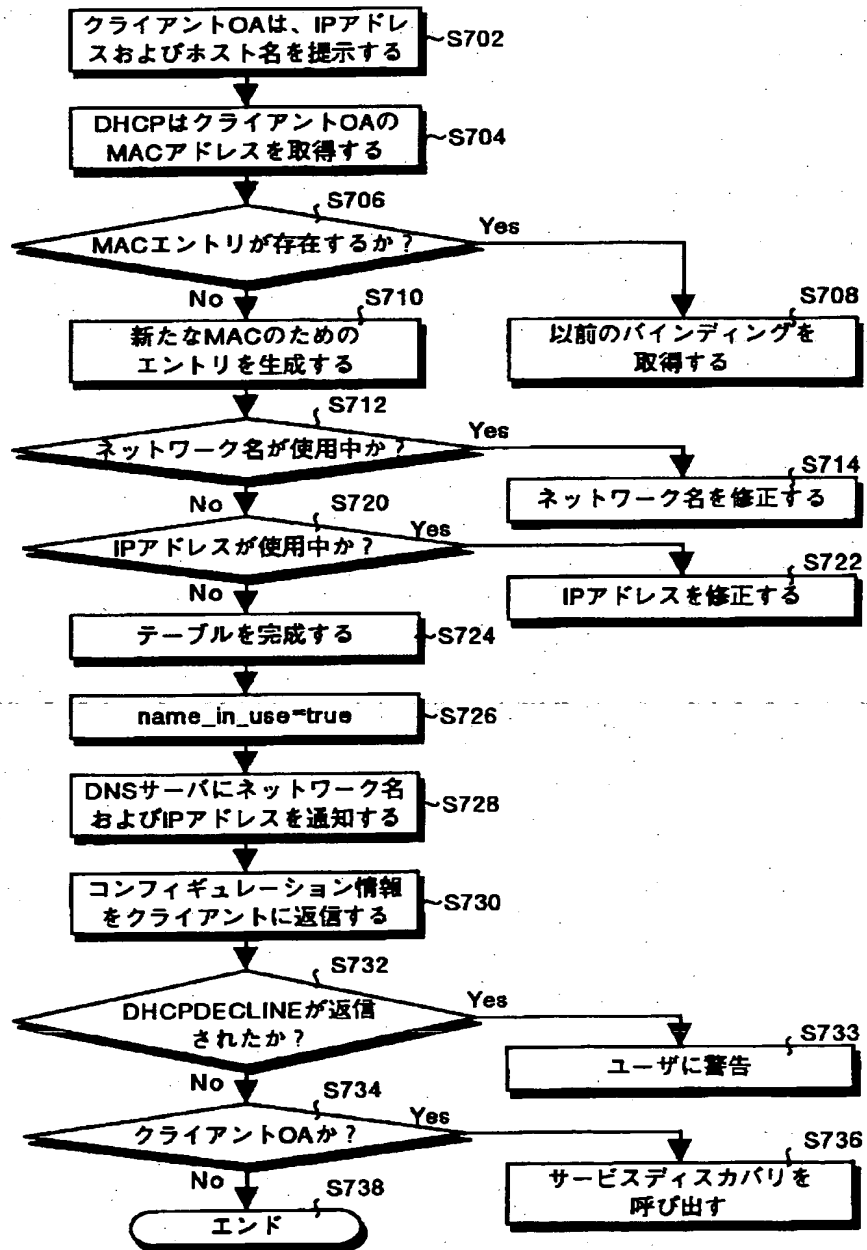
【図4】



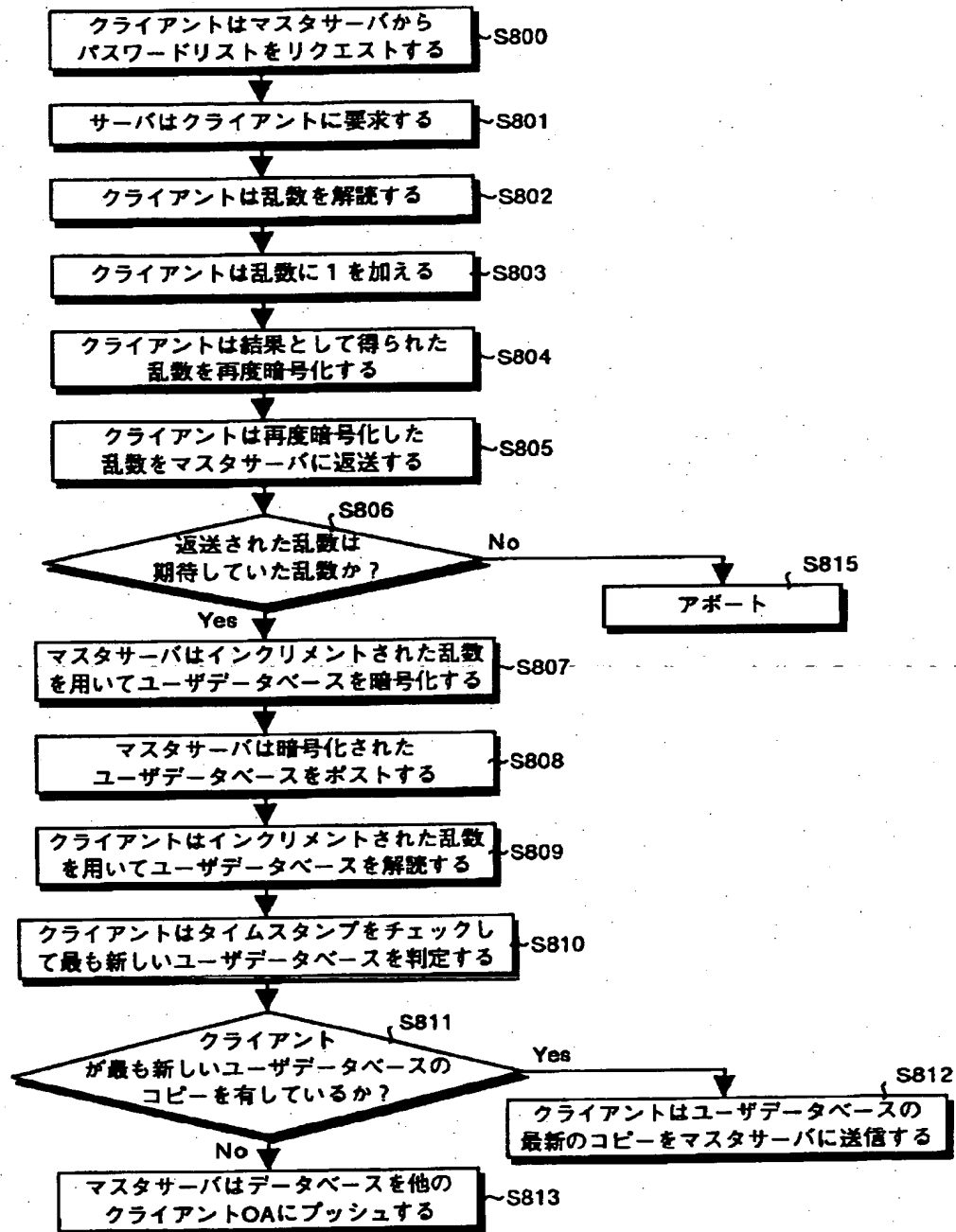
【図5】



【図8】



【図9】



## フロントページの続き

(72)発明者 カート ピアソル

アメリカ合衆国, カリフォルニア州

94025, メンロー パーク, スウィート

115, サンド ヒル ロード 2882, リコ

ー コーポレーション アール・エス・ブ

イ内

(72)発明者 寺村 信介

東京都大田区中馬込1丁目3番6号 株式

会社リコー内

(72)発明者 ト部 章男

東京都大田区中馬込1丁目3番6号 株式

会社リコー内

(72)発明者 稲垣 達也

東京都大田区中馬込1丁目3番6号 株式

会社リコー内